Should I get a security certificate for my web site?

This is no longer an option, the answer is “yes”.

What is a secure certificate?

A secure certificate is a digital “document” that is applied to your internet domain name on the server that provides various internet services, most importantly hosting your web site. You may encounter references to an **SSL certificate**, same thing.

What does it actually do?

The effect of having a certificate installed is that data transferred between the end user and the web server is encrypted.

In theory a determined third party could read unencrypted traffic (it's not easy unless you work for GCHQ or the CIA).

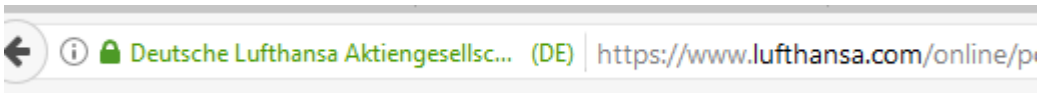
In most web browsers a secured site will show a locked padlock icon. Without a certificate most show an unlocked padlock. Google Chrome now shows the text “Not secure” instead of the unlocked padlock. These alerts are likely to become more common and more prominent in future, further increasing the desirability of having a secure certificate.

Most web sites have managed for over 20 years without and SSL would still be unnecessary but for some policy changes, mostly by Google at present.

What does a certificate cost?

The cost depends on the type of certificate. Sites handling confidential data need higher levels of certificate. That is more expensive, maybe £500 p.a. but a more significant issue is that implementation is trickier. It’s an unnecessary expense for most small & medium businesses. All but the largest businesses pass transaction handling to a PSP (Payment Service Provider such as SagePay, PayPal or WorldPay).

The more expensive EV (Extended Validation) certificates look like this in the web browser:



The cheapest commercial certificates might only cost £30 p.a. and are less difficult to obtain and install, many providers ask a much higher price for the same thing.

There are now free certificates available (under the banner "Let's Encrypt"). Many web hosting providers will now (on request) add a free certificate to your internet domain name.

WARNING: Don’t have a certificate installed without knowing how to make the other changes to the web site that are often necessary.

- Free certificates are provided on demand, the only condition is that you demonstrate that you have control of the domain name in question by making a small change.

This document is copyright Laser Technik Ltd, a limited company registered in England and Wales.
Registered number: **09117428** Registered office: Laser Technik Ltd, 18 Hoober Rd, Sheffield, S11 9SF

- Visit Let's Encrypt web site at https://letsencrypt.org/, notice the high-profile supporters of the initiative.
- Most owners of web sites will need to call on some technical assistance and that may come at a cost.

My approach has been to add a certificate and make any changes required at no cost unless it was going to be complicated. I received a call from one of my clients for whom I'd implemented a free certificate, they were seeking advice. They told me, "Another web designer is asking for a setup fee of £350 and an annual charge of £100 to make each of our other web sites secure". Having established that they use a PSP and that their ecommerce package is SSL ready, only needing a trivial change to make it secure I advised him to seek further clarification/justification from the other designer.

Is the free "Let's Encrypt" certificate good enough?

- It is only the data in transfer that is encrypted, what the web site then does with that data may still be insecure. That's true even of the most costly certificates.
- Free certificates are provided on demand the only requirement is that you can demonstrate that you control the domain name in question. The low-cost certificates require little more.
- Let's Encrypt is considered good enough for Shopify to implement it by default for the over half a million online shops on their platform: https://www.shopify.com/blog/73511365-all-shopify-stores-now-use-ssl-encryption-everywhere

How does a certificate benefit me as a web site owner?

At first the benefits are in Google Search and Google Chrome web browser but more will follow.

The most visible impact is that your web site will show a padlock icon on the address bar and the underlying complete address will change from http://example.com to https://example.com That's been the case for many years with little impact but that is changing.

That visible evidence will instil greater confidence in your site by visitors. An added incentive for having a certificate is that Google search now exhibits a preference for secure sites.

The biggest risk of not having a certificate is that visitors to your site will be scared away by the "Not secure" warning in their web browser. Further alerts may pop-up when a user attempts to enter text in any forms on your web site – even a simple search box.

If yours is an ecommerce web site you may have relied on passing the payment process to a secure third party PSP. That is no longer enough, you need a certificate as well but Let's Encrypt is good enough.

So why aren't all web sites secured?

In brief – now that cost isn't an issue it's just a matter of time. For some older sites there may be a problem with the technology behind the site requiring a significant rebuild. It's very likely that within a couple of years only old and poorly maintained web sites will remain insecure.

This document is copyright Laser Technik Ltd, a limited company registered in England and Wales.
Registered number: **09117428** Registered office: Laser Technik Ltd, 18 Hoober Rd, Sheffield, S11 9SF

I've got a certificate but I'm not seeing the padlock icon.

That implies that the website is misconfigured. In such instances instead of the unlocked padlock icon you may see some other indication of a problem (e.g. a padlock in a yellow triangle) indicating that the certificate has been applied but there is a technical problem needing attention.

But surely the commercial certificates are better

The more costly ones deliver higher grade encryption and the EV

In summary:

There is no longer any reason why every web site should not obtain a certificate. The benefits of doing so are becoming more significant.

Anyone creating **a new web site** today would be failing if they didn't obtain a certificate. In most cases the cost should be small or zero.

For sites handling sensitive personal data it may be necessary to consider commercial certification. That needs to be part of an overall security strategy to ensure data remains secure once it reaches the server.

For **existing web sites** you still need to get certification but the implications of a switch may be greater.

- The issue is not "should I obtain a certificate" but how, when, and what are the implications.
- Does your web host provide Let's Encrypt certificates? If not it's time to find another provider.
- Does your web designer know how to implement the certificate – and at what cost?
- An existing ecommerce site will very probably already be using a secure PSP (payment service provider). Large organisations like national supermarket chains will have a costly high grade certificate so as not to need a PSP (because the PSPs take a small percentage of each transaction).
- For sites handling sensitive personal data, certification should be part of a wider security review. Take the opportunity to check no other issues need addressing.

This document should not be regarded as definitive, there are some simplifications.

This document is copyright Laser Technik Ltd, a limited company registered in England and Wales.
Registered number: **09117428** Registered office: Laser Technik Ltd, 18 Hoober Rd, Sheffield, S11 9SF