conscious

brand, design & marketing for law firms

Go Secure with HTTPS

Prepared by

Bryony Cole (Product Manager)

Conscious Solutions Limited

Royal London Buildings

42-46 Baldwin Street, Bristol, BS1 1PN

Tel: 0117 325 0200

Email: sales@conscious.co.uk

Web: https://www.conscious.co.uk

Table of Contents

1 Overview

HTTPS has been around since 1994 and was originally used for online payments, login areas or sites asking for sensitive information. However, since Google announced that HTTPS was going to become a ranking factor in 2014[1] the number of sites using this protocol has increased dramatically, with Mozilla reporting that 50% of the web is now encrypted[2].

2 Benefits

2.1 SEO – HTTPS is a Ranking Factor

As mentioned above, Google has been a driving force for sites going HTTPS based on the incentive of higher rankings, saying in 2016:

> ***"We'll continue working to ensure that migrating to HTTPS is a no-brainer, providing business benefit beyond increased security."*** [3]

Converting to HTTPS also gives you more accurate analytics data as the referral data from a secure site may be dropped when the user crosses to a non-secure one.

2.2 Avoid Warning Messages from Chrome

On 18 August 2017 Google announced that from October 2017 users of Google Chrome V62.0 and above would receive warnings when entering data into forms on websites that are not fully secure. We have written about this in more detail on our blog but since Chrome is now used by over 50% of people this is yet another reason to go secure.

[1] https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html

[2] https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web

[3] https://webmasters.googleblog.com/2016/11/heres-to-more-https-on-web.html

2.3 User Experience

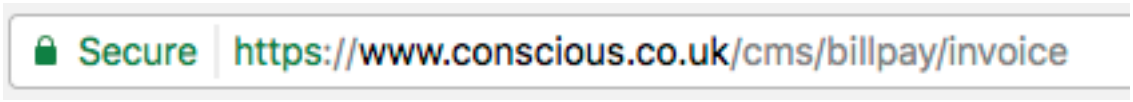
As the number of secure sites increase, users are paying more attention to the browser indications, especially when filling in forms. Comments like this one are not unusual:

> ***"I couldn't accept the online quote as the web-page is insecure and we don't feel comfortable submitting personal details without https. We hope you understand."***

If a potential client does not trust your site, they will not fill in a form. There are many ways of building this trust through the design and content, but users are also becoming more aware of cyber security and looking for the HTTPS indicator.

Some of our modules require a secure area. If you run our Billpay module for example, you may have noticed the client gets transferred to the Conscious secure site before entering any details.

Once you have your own secure certificate you are able to stay on your sites domain, increasing your clients trust in the site.



2.4 Security

You may have expected to see this top of the list, but it's important to understand that the encryption that HTTPS is only a part keeping your site safe and is designed to protect the user rather than your server.

Encryption offers a solution for two types of attacks:

- Privacy / Sniffing - the communication between the website and the user being monitored
- Identity / Phishing - your site is copied, users directed to the fake site and asked for personal data.

With HTTPS the user can be sure that the site they are using is actually you. However, keep in mind that although you stop hackers from seeing the interaction between the user and site, data sent via email, for example through forms on the site, is not covered by this encryption.

3 Certificate Options

3.1 Types of Certificate

There are three types of certificate, DV, OV and EV. There is no difference in the secure technology behind the types, but the checks done by the Certification Authority issuing the certificate are more robust for OV and EV and include business information.

Organization Validation (OV) – Recommended

The Certificate Authority reviews multiple databases and performs manual checks to confirm the business and applicant details. As with all certificates, the address bar in the browser is altered to highlight the site is encrypted.

Extended Validation (EV)

The Certificate Authority completes extensive checks into the business and authority of the applicant based on the Certificate Authority/Browser (CA/B) Forum guidelines. This certificate level has a different appearance to the OV and DV options, showing the companies name.

Domain Validation (DV)

Although this provides the same level of encryption as OV and EV certificates it is intended for personal sites and blogs rather than business sites. The Certificate Authority uses the WHOIS database to check the information matches the application. There is no difference in the way the browser shows the padlock icon however if you view the certificate there is be no organisational data.

3.2 Certificate Providers

We use SecureTrust (a division of Trustwave) for all our certificates. The cost of the certificates varies by type and the length (you can choose 1 or 2 years). We recommend an OV certificate for 2 years.

	OV (SSL Web Server)	EV (SSL Web Server with EV)
Two Years	$314.98	$466.20
One Year	$174.99	$259

Prices in the table above are correct as of 1st June 2019.
To see current prices please visit https://certs.securetrust.com/buy-ssl-certificate

If you are interested in using another provider, or would like to discuss using a DV Certificate, please contact your Account Manager. You may also want to read our blog The Cost of a Cheap HTTPS Certificate.

4 What Will it Cost?

The cost of converting your site to HTTPS has several components.

4.1 Conversion Cost: £400

This covers the work to upgrade your site and the move to our HTTPS platform including all the necessary redirects and a fully range of testing.

4.2 Hosting: A minimum of £60 a month

Our hosting package for the HTTPS platform starts from £60 a month, please contact your Account Manager to discuss your existing charge for hosting and to confirm if your total monthly cost will be affected by the move from http:// to https://.

4.3 Certificate Cost: Variable

Costs vary based on the type and time period you purchase them. See table above.

5 The Process

5.1 Information Required

We handle the application for the certificate on your behalf. To do this we require the following information:

- Legal Name of the company
- Contact Name (Who knows they will be contacted by the Certificate Provider)
- Job Title of the contact
- Company Address (inc County) - This needs to be publically verifiable and should be the head/registered office.
- Company Phone Number - This needs to be publically verifiable
- Email Address of the contact
- Your choice of certificate (provider, type and length)

When suppling this information you should keep in mind that:

- Details must be 100% accurate or the certificate may not be issued and may incur extra costs to correct.
- 2 year certificates are cheaper than 1 year certificates
- By default the certificate will be for the main domain only (with and without www.) Redirected domains can be added to the certificate but will incur an extra charge. If you want to include these we need to know before we make the application

5.2 Initial Checks

Before we apply for the certificate we carry out a number of checks by converting your test site to HTTPS.

The main elements we are checking for are Iframes. These are other sites embedded in the site (e.g. Google Maps and YouTube videos). These need to come from an HTTPS site or the browser will block the content and show a warning.

Images are also sometimes handled in this way (Chambers and Legal 500 logos in particular), so we also need to check these are accessible from an HTTPS site, or add them directly to your site instead.

These checks are done on the test site to give us an overview of any changes that will be needed when we convert the live site. The test content will not replace the content on the live site.

We also check your record in the WHOIS database. This gives the details of who your domain name is registered to. This information must match the current company name and address as part of the certificate checks. We often find that the name is slightly different (missing Ltd or LLP) and in some cases are registered in an individual's name instead of the company. We will let you know if we find a problem and ask you to update this before we apply for the certificate.

5.3 Application

Once we are happy with the checks we will apply for the certificate.

Within a couple of days, the contact you have given should receive an email asking them to verify the application. If they are asked questions about the company the answer must match those that have been given for the application.

The contact may also receive a call through the switchboard to verify their identity and the HR department may be contacted to verify their position.

5.4 Live Site Conversion

When the application has been approved we will be notified directly. We will then contact you to book in a conversion date for the live site. This can usually happen within a week of the approval.

In order to complete the process, you will need to change the A-Record in your DNS settings. This can take up to 48 hours to complete from the point it is changed. Once we convert the live site the site will not be editable through the CMS and any module that requires a secure area will not be usable (Billpay, Extranets) until the A-Record change is complete. It is therefore important that we time this correctly to be as non-disruptive as possible.

We will convert the live site at the agreed time and run our final checks, then ask you to action the A-record change. Alternatively, you can supply us with the login details and we can make the change for you.

We also add a redirect rule so that anyone trying to access the page using a http:// address gets automatically taken to the matching https:// page.

Your site is now fully secure. Any modules and the editing system are now functioning as before.

5.5 Update any SEO Tools and PPC Campaigns

For the best results these will need to be updated to point to the HTTPS domain. We will update any we are running for you, but if you run your own or use an external agency you will need to get these changed.