SSL & HTTPS Explained for Business Owners

Why website security matters

- Most people will first see a business's website before contacting the business.
- When visiting a website, users expect the site to load quickly, be visually appealing, and be safe to use.
- The way websites establish a secure connection is through HTTPS, which signifies that a web page can be trusted to protect information transmitted over the Internet.
- Web browsers will display a lock symbol in the address bar for websites that utilise the HTTPS protocol.
- By encrypting the data being sent between a user and a website, HTTPS protects sensitive information such as names, addresses, and credit card numbers.
- An SSL Certificate provides the underlying security features necessary to encrypt the data being transmitted.
- The majority of modern web browsers will typically display warnings to users that attempt to connect to an unsecured site utilizing the HTTP protocol.
- When searching for a site to visit via a search engine like Google, websites using HTTP are not ranked as highly as those using HTTPS.
- Therefore, implementing HTTPS on a website establishes credibility with customers and builds trust with visitors.
- As of 2026, implementing HTTPS on a website is considered the minimum requirement for businesses to continue doing business on the web.

What is SSL

SSL is the abbreviation for Secure Socket Layer. SSL is a technology that gives customers a private (encrypted) connection between their browser and your website.

To demonstrate how secure SSL technologies are, imagine sending a letter via normal post where anyone can open the envelope and read the contents. SSL works by putting the letter in a tamper-proof box with a lock, where only the intended recipient can open it. This way, the information travels without risk of being read or altered before it arrives at its final destination.

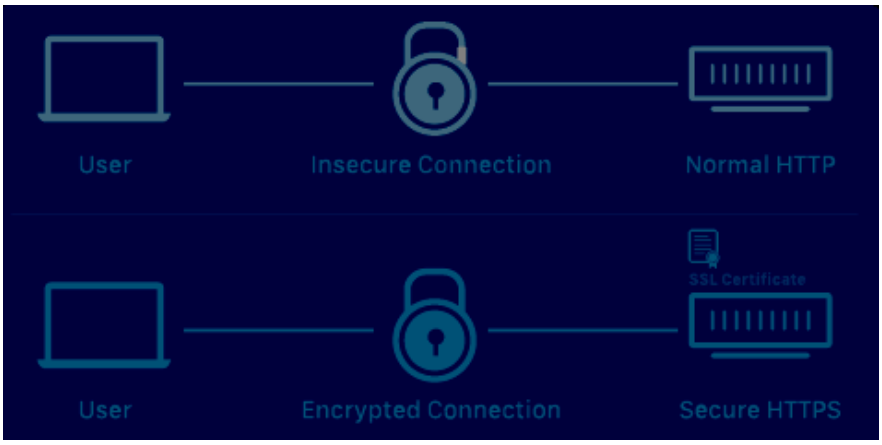
SSL is the technology - HTTPS (HyperText Transfer Protocol Secure) is what you see when it is in action (the 'S' in HTTPS stands for secure).

What HTTPS means

HTTPS is a way to tell customers that you have an SSL certificate installed, which means that your website is using SSL technology to provide encrypted connections. To see if a website has an SSL certificate, you will see:

- The web address starts with https:// rather than http://
- There is a padlock icon at the beginning of the web address
- There are no security warning messages being displayed by the browser

When a customer fills out a contact form, enters payment information or logs into a customer area on your site, HTTPS scrambles that information so that only your website can decipher it.

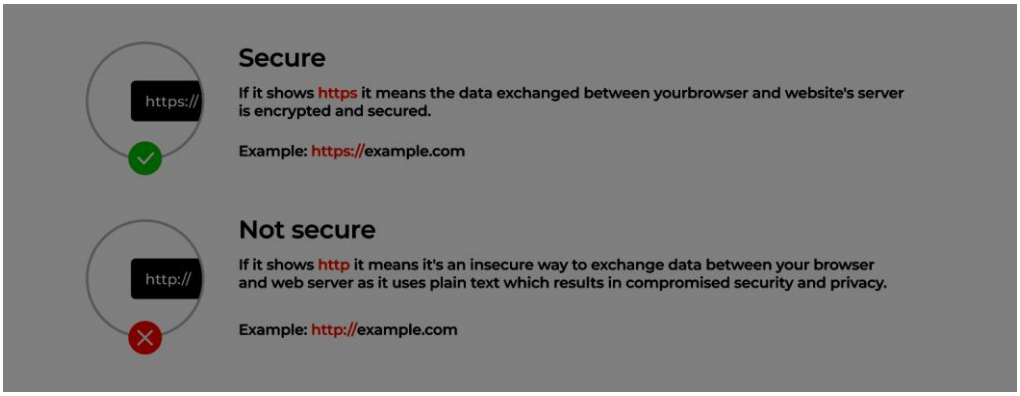


Difference between HTTP and HTTPS

HTTP is less secure than HTTPS: With HTTP (old version), your data is transmitted over the internet in plain text. Anyone who can intercept your data travelling through the air(Wi-Fi) while you're on a public Wi-Fi connection can read or modify it. Browsers will flag HTTP sites as "not secure."

HTTPS protects your data while in transit and helps protect your private information, such as credit card numbers, physical addresses, and other sensitive information by encrypting your data. Even if someone were able to intercept your connection, they would only see a jumble of characters and would be blocked from changing any information because they would have no key to decrypt it.

As of 2026, most reputable websites use HTTPS; Google gives HTTPS websites a modest boost in search engine results; and many consumers will abandon their purchases after seeing a "not secure" error message on your website.



How SSL protects website visitors

SSL protects 3 key areas:

- **Confidentiality:** SSL protects your data while it travels over the internet so that nobody can see your credit card number or address before they reach its destination.
- **Integrity:** SSL protects your data while it travels so that you can be sure nobody has changed it before it arrives (for example, nobody can change a bank account number in a payment transaction).

- **Authentication:** SSL helps you establish the authenticity of your website and ensures that visitors have confidence they are visiting your legitimate website and not a counterfeit site established by a criminal.

Thus, for UK businesses, secure sites encourage customers to share data and may increase conversion rates and decrease form abandonment rates.

Types of SSL certificates explained simply

There are several main kinds of SSL certificate, but most of the differences are simple to understand for the average UK small business. Here's a quick summary of all the types available in 2023.

- **Domain Validation (DV) SSL Certificate:** This is the most common and cheapest type of SSL certificate. DV certificate validation simply verifies that you own the domain name that you used to apply for the certificate. This makes them ideal for brochure-style websites and smaller retailers.
- **Organisation Validation (OV) SSL Certificate:** An OV certificate verifies that your business is registered with Companies House in the UK (or equivalent) and can be relied upon. These SSL certificates provide more trust for clients or consumers, and are usually required on service-based websites.
- **Extended Validation (EV) SSL Certificate:** With the EV certificate, your business will be prominently displayed in a green padlock or domain name within the address bar of the majority of browsers. The EV certificates are predominantly used by banks or very large e-commerce sites, and are seldom required for most small- to medium-sized businesses.
- **Wildcard SSL Certificate:** A wildcard SSL certificate is a single certificate that can be used to secure the primary domain (for example, yourbusiness.co.uk) along with any subdomain(s), including shop.yourbusiness.co.uk and blog.yourbusiness.co.uk.
- **Multi-Domain SSL Certificate:** A multi-domain SSL certificate enables you to secure multiple distinct domain names with a single certificate (for example, yourbusiness.co.uk and yourbusiness.com).

An average small UK business should have no problem being able to obtain a DV SSL certificate from either Let’s Encrypt (free) or from their web site hosting provider for a nominal fee.

How businesses obtain and install SSL certificates

Most modern hosting providers have made obtaining and installing an SSL certificate easy:

- **Automatic with Hosting Providers:** Most UK Hosting providers (Site-Ground, Krystal, Heart Internet) now include free SSL with Let’s Encrypt and will automatically configure it when the account is created.
- **One Click Install:** For most hosting providers where the automatic option is not available, there are buttons in the hosting Control Panel that will install a free SSL.
- **Manual Install:** If you need to manually install an SSL certificate, your hosting provider or developer can do so within minutes.

Once you have installed your SSL, users should automatically be redirected from HTTP to HTTPS. You can verify this by typing your domain name with a "http://" and checking to see if it automatically redirects to "https://".

Common SSL mistakes businesses make

- **Still Speedy HTTP:** While your website will still load, users will receive a warning indicating it is currently "Not Secure".
- **Old Certificates:** If you have expired SSL certificates on your website, users will receive warnings that "This site uses an expired SSL certificate".
- **Mixed Content:** Some images or scripts may still be loading through unencrypted HTTP rather than encrypted HTTPS.
- **Failure to Renew Automatically:** Once you have let your SSL certificate expire, there will be warnings on your website until it has been manually renewed.

Website HTTPS security checklist

- ✓ Is your site secured with an SSL certificate that displays padlock symbol when secured?
- ✓ Is your site automatically redirected from HTTP to HTTPS?
- ✓ Are all images, scripts and other resources being pulled from a HTTPS source based on how your instructions were provided to the server?
- ✓ Does your SSL certificate meet all current and future SSL requirements?
- ✓ Does your SSL certificate cover any/all sub-domains associated with your main URL?
- ✓ Are customers informed via alerts or signs on forms and during the check-out process?

SSL certificate management checklist

- ✓ Is SSL certificate currently installed on my site and working properly?
- ✓ What is my SSL certificate renewal date, and can I set the certification to auto-renew?
- ✓ Is my SSL certificate type appropriate for my site?
- ✓ Is there any mixed content associated with your site (www versus non-www)?
- ✓ Is there a monthly check performed to confirm that the site URL contains a padlock symbol?

Website security best practices checklist

- ✓ All pages use HTTPS (are SSL secured).
- ✓ Admin area is secured with both strong passwords and an active multi-factor authentication system.
- ✓ Software update cycles for CMS/Plugins are completed timely.
- ✓ Basic firewall or security plug-in is enabled/active.
- ✓ Backups are performed and/or tested at least bi-weekly.

✓ A privacy notice and cookie consent statement are actively placed on site where applicable.

FAQs

1. Has SSL continued to exist as of 2026?

Yes, because it is considered to be the norm now. HTTP sites receive a warning upon entering via a browser and Google has a preference for HTTPS sites when it comes to rankings.

2. Is it required for all websites to have HTTPS?

Yes, all websites, including one-page "brochure" style websites. It establishes credibility and allows access without being warned about it by your browser.

3. What is the cost of purchasing an SSL Certificate?

Most hosts include a free Let’s Encrypt certificate; however, you can purchase one from a business that costs approximately £10-£50 per year.

4. Are certificate-installation agencies able to include SSL functionality in their website building platforms automatically?

Currently, there are several web-building platforms like Wix, Squarespace, Shopify where the user receives free SSL certificates automatically.

5. What will happen if the SSL certificate for my website expires?

Users will see warnings about the website being insecure or untrustworthy and may leave. Users may continue to view the page but it may not be perceived as credible.

6. To operate an e-commerce type website do you require an SSL Certificate?

A standard DV certificate should suffice for most payment providers that process credit card transactions securely.

7. To verify if your website has SSL (HTTPS) installed?

You can check this by entering your domain name into a web browser. Look for a padlock icon next to the address bar, which will indicate that your website is secure (i.e., using SSL).

8. Will having an SSL certificate have an impact on your site’s speed?

Modern-day implementation of SSL does not hinder performance and with HTTP/2, may actually improve the performance of your website.

9. What should you do to fix mixed content issues on your site?

You should replace images, scripts and links that reference (http://) HTTP with (https://) HTTPS. Most hosting companies and content management systems will provide this option.

About This Guide

The Computer Support Centre has created this guide to help business owners comprehend how critical it is that they protect the security of their websites as well as the role of SSL and HTTPS in safeguarding information online. Many businesses utilise their website as a means of interacting with customers, gathering enquiries, and completing transactions; therefore, it is vital for the business to have secure connections when communicating with customers.

The purpose of this guide is to clarify the basic principles that govern the operation of SSL Certificates and HTTPS Protocol, outline why it's imperative to protect customer data using these technologies, and provide guidance on the implementation of these technologies. The guide also provides real-world examples of common errors businesses make when establishing website security, as well as security best practices and checklists that organisations can use to ensure that they have an effective and trustworthy online presence.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

All 21st-century businesses have an online presence, thus securing your website should be a priority. A website can be secured by utilising the HTTPs protocol, which can be established by purchasing an SSL Certificate from an authorised SSL Certificate Provider, so you can enable the HTTPS protocol for your business.

For many businesses, it is relatively easy to implement HTTPS on their website, and many modern hosting services automatically provide this feature. Businesses can eliminate browser alerts and maintain customer trust by having an automated renewal process for their SSL Certificates and ensuring that their SSL Certificates are installed properly.

As of 2026, businesses can no longer afford to overlook having a secure website, as secure websites have become essential to having an online professional and respectable business. Using this article as a guide, businesses can protect their sensitive data from prying eyes, provide reassurance to customers that their information is safe with you, and maintain a reputable online presence.