WHAT IS A SSL CERTIFICATE?

WHY A BUSINESS WEBSITE SHOULD HAVE ONE.

Everyone has heard about the website security problems that businesses and institutions face on the Internet.

Organisations from government departments like the NHS, to small businesses are affected by hacking attacks from time to time, so safeguarding of customer data and business data is extremely important.

Nowadays, the best way to make a website more secure is with a SSL certificate.

BUT WHAT DOES A SSL CERTIFICATE DO?

An SSL certificate is a piece of software code that establishes a secure connection between the user's browser and a website.

You can see the SSL in action on the most popular websites on the Internet. For example, go to Google or Facebook. You can see two things in the address bar of your browser that show that these websites have made a secure connection between their web servers and your browser.

1. HTTPS:

The first part is the URL of the web page. Standard websites start with HTTP, but sites that have an SSL certificate add "S" to it, making it HTTPS. Which means all data between the user and the website is encrypted.

2. PADLOCK

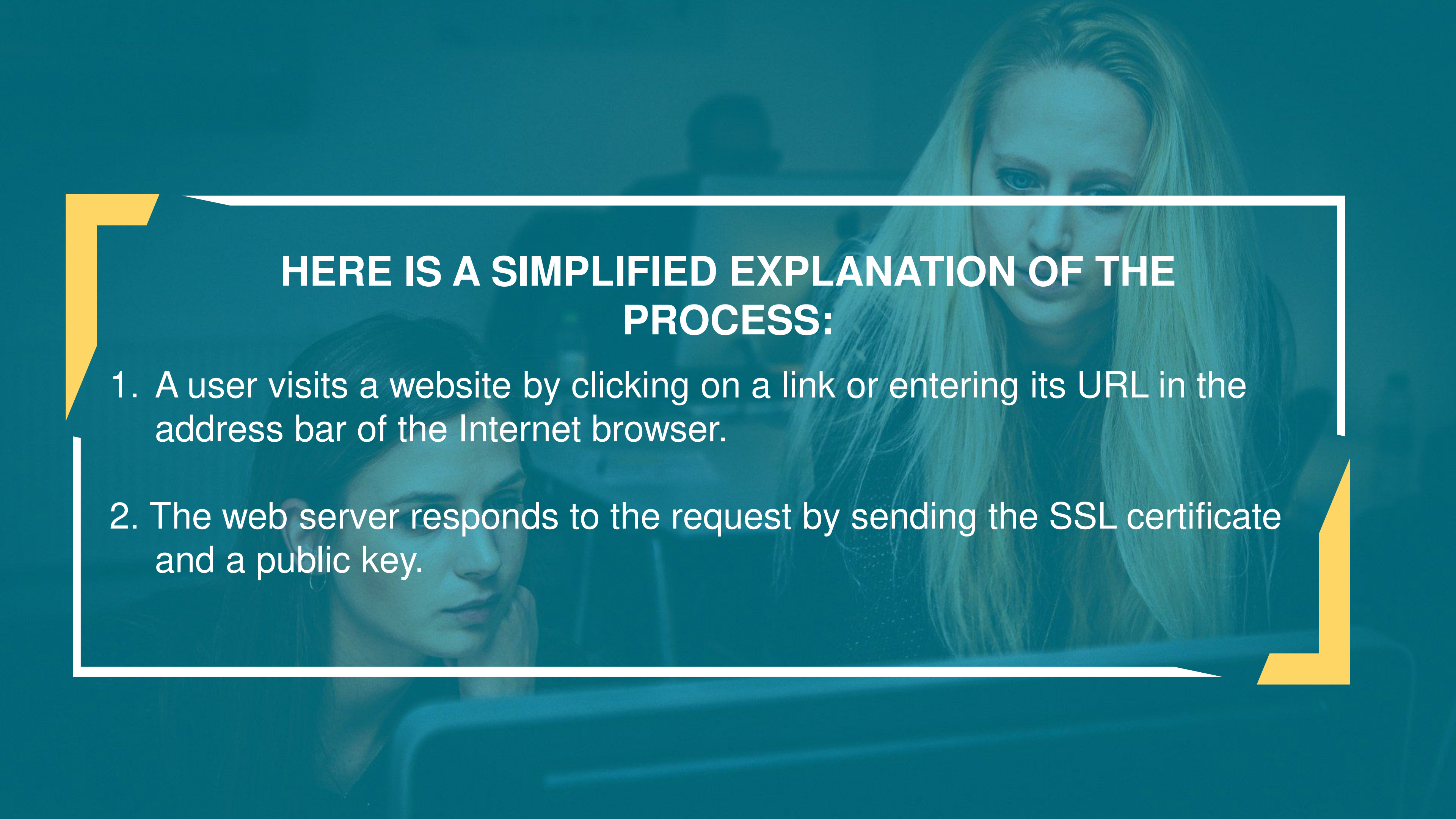
You will also see a closed padlock in the browser's address bar, somewhere next to the address of the web page.

A company still needs to have Firewalls and Anti-Virus software install on all the company computers. Email attachments from unknown sources should never be opened but referred to the IT department.

HOW DOES SSL WORK?

SSL means Secure Sockets Layer and it works by encrypting the connection between a user’s browser and the website server.

To make it work on your website you need an SSL certificate.



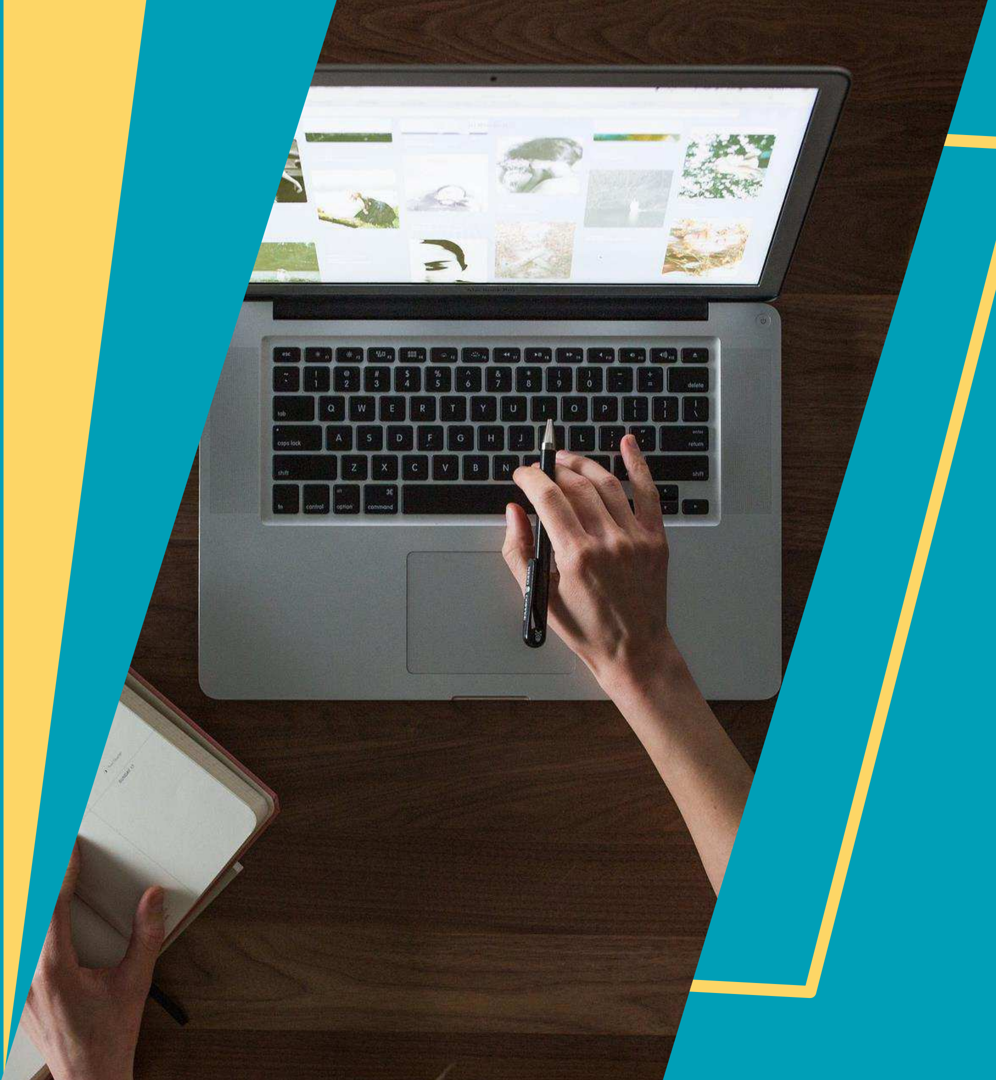
HERE IS A SIMPLIFIED EXPLANATION OF THE PROCESS:

1. A user visits a website by clicking on a link or entering its URL in the address bar of the Internet browser.

2. The web server responds to the request by sending the SSL certificate and a public key.

3. The user's browser checks the certificate and then uses the public key to create an encryption key, which is sent back to the website server.

4. The server decrypts this and shares the request (processes a payment, loads a web page, connects to a web page, etc.) and sends the information to the user's browser with the encryption key.



5. The user's browser decrypts the information and displays it on the screen.

6. The whole process lasts a fraction of a second, but it ensures that a secure connection is established.

WHY IS A SSL CERTIFICATE IMPORTANT FOR ALL BUSINESSES?

SSL certificates secure the data sent between the server and the user's computer in a way that cannot be manipulated.

For example, when you type a search term into Google, it's impossible for anyone to spy on the phrase you're looking for. Similarly, when logging into Facebook, it is not possible to intercept and decrypt the password while it is in transit between the computer and the Facebook servers and when the payment information is sent to PayPal or a bank, a hacker cannot access your credit card or bank details while the transaction is taking place.

SECURE DATA TRANSFER:

Internet users have come to trust SSL certificates, in part, because of how they are created. They are issued by certification authorities.

These companies have a root certificate that is pre-loaded in the most common web browsers, such as Chrome, Internet Explorer, Safari, and Firefox. This means that the developers of the browsers (Google, Microsoft, Mozilla) know and recognise the certification authority as a reliable source of SSL certificates.

The first benefit of SSL certificates is evidenced in its main objective. That it is to keep the communication between an Internet browser and a website server secure.

If your website doesn’t have an SSL certificate it’s possible that other people are able to access the data shared between the website servers and the customer’s browser.

This information could be the details of a customer account, customer’s username and passwords, customers address, names and even credit card numbers or other sensitive information on your website that you have stored in the database.

When you have the SSL Certificate installed on the web server, all information is encrypted and can only be read from the server by authorised persons and the internet browser that receives the data and have the key to decrypt it.

Considering the above, it is clear that SSL Certificates are able to protect and safeguard client and customer information.

BUILDING TRUST WITH CUSTOMERS:

Another advantage of SSL certificates is that as the security of the website and the business are improved, customers become more confident of being on the website and making purchases. With the SSL Security Certificate, companies can avoid data theft by guaranteeing customers completely security of purchases.

Greater customer confidence means the possibility of increased sales.

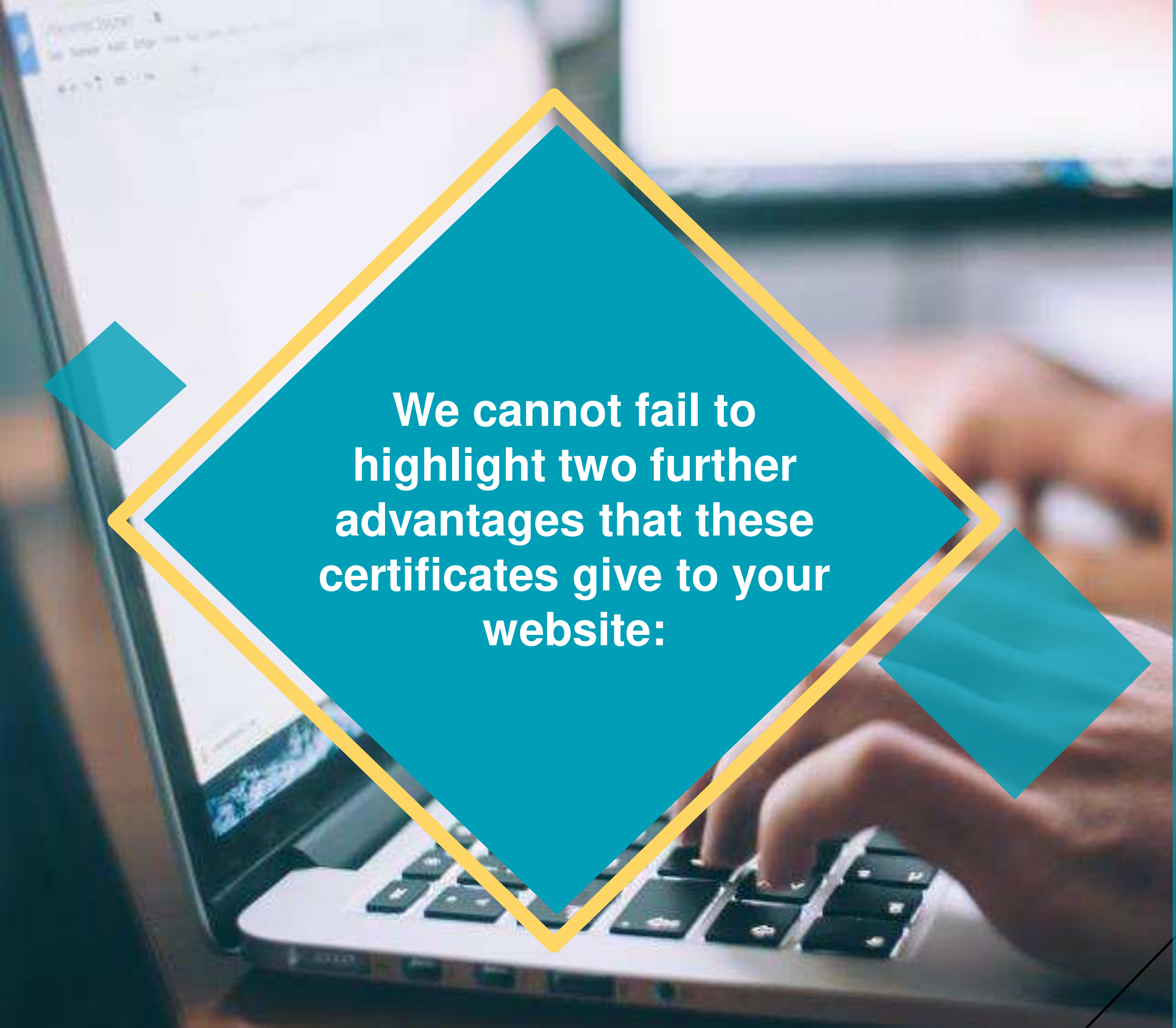
With the SSL Certificate you can also certify the identity of your business, proving that you are the one who manages the information. A business presents itself with a more reliable identity and make users trust a business.

RANK BETTER ON GOOGLE:

In terms of optimisation in search engine optimisation (SEO), website owners should bear in mind that Google values this type of certificate positively, and about 40% of top ranking sites already have a SSL certificate installed.

Even though it’s still a very small ranking factor, having a SSL certificate on your website can help you improve the ranking on your website on Search Engines, especially if your competitors don’t have one installed on their website.

With improved ranking, you can increase traffic without additional costs.



We cannot fail to highlight two further advantages that these certificates give to your website:

Authentication and Privacy. When a website has a SSL certificate, the business owner is validating their identity and users entering the website know that a business is really correct, and not a third party.

In addition, the privacy provided ensures that the data transferred between a website and customers cannot be read and used by others.

This is needed to comply with the **EU Data Protection laws such as GDPR** effective 2018.