

Quick guide to website security

Essential website security tips
for your growing business



Quick guides for growing businesses

it'seeze websites
Helping your business grow

Growing your business, securely

When you're creating a website for your business, it's always worth making security a priority. Getting it right will not only keep your data - and your customers' data - safe, it will also help you make sure you don't fall short of your regulatory obligations. After all, nobody wants to face a hefty fine because they didn't take GDPR seriously. (Not sure how GDPR applies to you? Don't worry... we'll get you up to speed).

This quick guide will help you understand the key security features your website needs and how they protect you and your customers. It also outlines the crucial role that security certificates play in improving your Google rankings and getting your growing business seen online.

This guide covers:



SSL certification



Secure Hosting

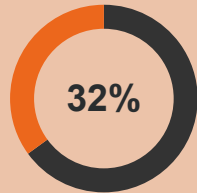


Compliance

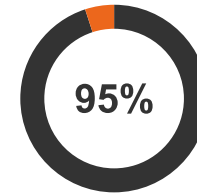


Staying up to date

Every website needs **security**



FACT: 1/3 of businesses were hacked in 2019*



FACT: A hacked and blacklisted website can lose around 95% of its traffic**

Never believe that your website is too small to face a security threat. While larger sites may be a more appealing prospect for hackers intent on sabotage or information theft, smaller sites also offer opportunity. Some fall prey to malicious attacks for little discernible reason. If your website is targeted, it may damage trust in your business and have knock-on effects for your growing brand reputation. Down-time and resulting short term revenue losses will only be one part of the problem.

The four essential considerations for keeping **your website safe**:



1. SSL certification

Important because: it keeps your data safe, boosts your search rankings and lets users know they can trust your website.



3. Compliance

Important because: it gives your customers the protection they deserve and prevents you from facing non-compliance fines.



2. Secure hosting

Important because: it keeps your data safe and affects the load speed of your website.



4. Staying up to date

Important because: security requirements (and threats) are continually evolving, making security updates an ongoing part of good website management.

1. SSL Certification



Every website that holds important information or asks for personal details should have a properly configured SSL certificate. SSL stands for Secure Socket Layer, but you don't really need to know that; what you do need to know is that an SSL certificate means all data travelling to and from your website is encrypted. Put simply, when your business is sharing information with a customer, or vice-versa, no one else can 'eavesdrop' on or alter the details being shared.

Importantly, having an SSL certificate for your website prevents users from receiving 'unsecure' warnings in their browser, which may put them off visiting altogether. SSL gives your website an 'HTTPS' connection, complete with a reassuring little padlock logo. This lets your customers know they can trust your site.

SSL also gives you a Google search benefit. You see, back in 2014, Google gave websites using SSL a 'ranking signal' to push them up the search rankings before non-SSL sites. That's invaluable for increasing your business' searchability.

In 2016, Google took this one step further when they updated their Chrome browser to explicitly identify websites without SSL as 'Unsecure'. All popular browsers will now give users an explicit warning when the website they are headed for is Unsecure. And unfortunately for those without SSL, most users are likely to abandon the site and head back to safety.

If you're an it'seeze customer and your website domain is registered through us, your website will have SSL certification as standard, containing the 'safe' green padlock icon recognised by Google, so customers will always know they can visit safely.

2. Secure Hosting

When choosing where to host your website, two things are important: server security features and physical location of data centres. Security features you should look for include SSL (see above), server monitoring, malware detection, tools that anticipate and block direct attacks, public key cryptography, and ongoing security updates to prevent any breaches and keep your website performing at its peak. The best hosting services will use servers that offer all of these as standard. They're crucial to protecting your business information and any personal customer data you store.



What's more important than you might realise is the physical location of the data centre you use. If you're a UK business, your ideal data centre will be located here in the UK. Using a UK data centre doesn't just make it easier to confirm that the right security features are in place and provide you with UK based contacts if things go wrong, it also provides better speed and reliability.

That's because although data is not a tangible thing, the infrastructure and power needed to store and transfer it are. Using a data centre located in a far-flung corner of the globe might provide a slightly cheaper option but may increase the chance of down-time and will inevitably cause 'latency'. This is a time lag between click and page-load; something which often causes users to abandon websites altogether.

If you're an it'seeze customer, your website will always be hosted by established and accredited UK data centres.

3. Compliance

Compliance requirements will vary from one website to another. For example, websites serving customers across the globe may need to comply with the legislation of more than one region. The primary compliance consideration here in the UK is the General Data Protection Regulation 2016 (GDPR). When GDPR came into force in 2018, it changed the way businesses were allowed to request, store and use customer data. GDPR is designed to give individuals more control over their personal and sensitive data.

It also creates a consistent law across Europe, making it easier for businesses to understand and adopt the right practices. GDPR was enacted in UK law through the Data Protection Act 2018 and will therefore be unaffected by our withdrawal from the EU. While we won't delve into [the finer details of GDPR](#) in this quick guide, we would recommend that all businesses seek professional advice on how the regulations apply to them.

A simplified overview is that you must now have a compliant privacy policy on your website, that you must always explicitly ask permission to store and use customer information, and that you do so securely, only keeping it for as long as necessary and only using it for the purpose agreed. You must also be able to completely remove personal records from your business if requested to do so. It's important to note that businesses of all sizes must comply with GDPR, even the very smallest. It's also worth knowing that fines for non-compliance are harsher than any seen in the UK for data-breaches before; GDPR allows fines of up to €20 million, or four per cent of annual turnover, whichever is higher.

If you're an it'seeze customer, your website will be GDPR compliant by design. This means we'll provide you with all the website essentials you need to help you comply with the latest regulations - including a privacy policy, cookie notice, and contact forms set up to protect sensitive data.

4. Staying up to date

Things move quickly in the digital world. The only way to keep your website working well is to stay abreast of new developments and, while this is important in terms of content, features and functionality, this fact is never truer than when talking about security. Security updates fix weaknesses and prevent hackers from exploiting those weaknesses to access your website's code or steal your data. As technology changes, hackers are developing new and more sophisticated ways to locate loopholes and identify vulnerabilities. Many now use automated 'bots' to scour the internet for opportunities - they cast the net wide and don't care if your business is large or small.



It's actually often the smaller businesses that become easy prey, as they are less likely to have made the latest security updates to their website. The damage that hackers can do ranges from defacing your website through to inserting 'black hat' SEO links to boost their website traffic - while damaging your own search engine rankings. They may also intercept valuable customer data or send spam emails to your contacts.

Any of these actions could result in your website being blacklisted and in your business losing the trust of its customers - but it's something you can prevent by treating security as an ongoing priority rather than something you do just once at the time of build. Invest in good security software for your website and even when your business is busy, remember that time spent installing system updates is always time well spent.

If you're an it'seeze customer, we'll always stay ahead of digital developments so you don't have to, and you'll receive the latest security updates at no extra cost.

We hope you've found this quick guide useful.

If you have any questions about how to make your website more secure, we'd love to help you find the answers. Why not get in touch?

Go to www.itseeze-windsor.co.uk

Call **01753 201204**

Email ann.naylor@itseeze.com

Security made simple, by it'seeze

it'seeze websites

Helping your business grow