IDEAL MARKETING

OWNING A BUSINESS WEBSITE 101

YOUR CONFIDENCE CHECKLIST

These days there are few businesses without a website. In fact, most businesses have had several versions by now, so the odds are you set up a lot of the components needed for a website years ago. But maybe you took the advice of someone you don't work with anymore, maybe parts of it were put together on a shoestring budget or perhaps the advice no longer applies as technology, best practices and security concerns have evolved. So, what are the fundamentals you need to know when running your website and where do companies frequently trip up?

Over the last decade we've built over 100 websites, mostly in the world's most popular content management system, WordPress. We've created everything from one-page websites to ecommerce, event booking systems, membership directories and learning management systems. Currently, we host over 70 on our dedicated server. So, it's safe to say we know a lot about the components of a website, where things can go wrong and best practices to keep everything on track.

The following is your business website confidence checklist. In this PDF we'll cover the following:

- Domain names
- Website hosting
- Website backups
- Website security
- Website notifications and company emails
- Privacy policies and cookie permissions

Why start here? Because our experience of managing a variety of websites created by a vast range of developers has taught us that getting these fundamentals right is the best way of avoiding the common pitfalls that can trip websites up. When a website stops working for you, it's confusing, frustrating and takes you away from running your business.

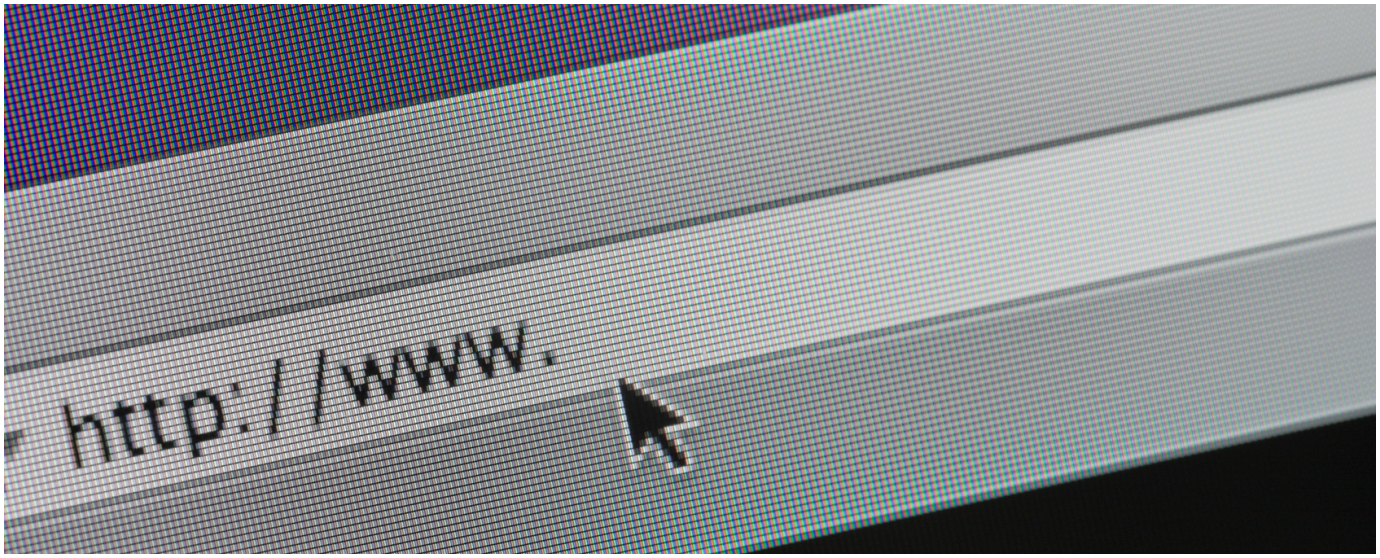
So, by taking these steps, you can ensure you're doing all you can to create a website that creates a pleasant and stress-free experience for both you and your customers.

DOMAIN NAMES

WHAT ARE DOMAIN NAMES?

In simple terms, your domain name is the address used to display the files that make up your website so that when someone types your domain name into an internet browser your website shows up. You can have multiple domain names, but usually you have a primary domain name where your website files are located and the other domain names are pointed at the website primary domain. For example if you have a domain name with .co.uk, .com and .uk at the end you might use the .co.uk domain as your primary domain and point the others to your primary domain. You might also buy similar versions of your domain name, with hyphens or because you can't pick the best option initially and so reserve a few so your competition can't have them.

It used to be that your domain name was a very important factor when it came to SEO and ideally, you'd want any keywords you wanted to rank for to feature in the domain name. However, search engine algorithms are much more advanced now, so don't get too bogged down if you're making a decision about what domain names to buy.



WHAT IS DOMAIN NAME BEST PRACTICE?

Take control of your domain names

Make sure you have control over your domain names via your own account as they are your intellectual property. Not having control of them can make it more difficult for you to move from your current website provider when it's time for a change.

When setting up a website, your website design company may have offered to buy your domain name for you to make things easier. However, in the long run it's better to have control, not least because your IT company will likely need access to update email settings.

If your domain name is hosted by your website design company, tell them you'd like to transfer it to your own account and ask what company it's currently hosted with. It's usually free to move your domain name between accounts as long as it's within the same domain hosting company. For example, if the domain name is current hosted in a 123-reg account, it's free to move it to your own 123-reg account, but if you had a GoDaddy account you may need to pay to move it from a 123-reg account to a GoDaddy account. There are dozens of domain hosting companies out there, but 123-reg, GoDaddy, Fasthosts, IONOS and Namecheap are some of the most popular. Once you know where your domain name is currently hosted, set up an account with the same company and follow their guidance to get things moved.

Ensure your domain names renew

If you do control your domain name, add your bank account as a payment method, not just your debit or credit card. As cards expire every couple of years, using one often results in a domain name renewal failing, which can result in the loss of your domain name. If you use your domain name for your business email this can be very disruptive as your email will just stop working, hampering your ability to operate and potentially damaging your reputation. So, setting up a backup method of payment of a direct debit means you're covered even if your card expires.

Buy variations of your domain name

Buy available variations of your domain name, particularly.co.uk and .com versions. This solves the issue of potential customers ending up on your competitor's website because they've forgotten whether your site is .co.uk or .com . This will only cost about £15 per year per domain, although the rate of domain names is subject to change and if you shop around, you may get a better deal.

Cancel unwanted domain names

If you follow the previous advice, you could also end up with domain names that are no longer needed and incur yearly unnecessary expense. Your domain hosting company should alert you before renewing your domain name, so in each case review if the domain name is still needed and cancel it if not.

Protect against account lockouts

Ensure that the email you use to login to your domain hosting account (held with companies like 123-reg, GoDaddy etc) IS NOT an email address connected to your domain name. As we've said, if you lose access to your domain name, your email will stop working and if you need to reset your password, you won't be able to.

WEBSITE HOSTING

WHAT IS WEBSITE HOSTING?

Your website hosting is where the files for your website are located. The type of hosting available is usually based on whether you have shared website hosting, a virtual dedicated server or a dedicated server. With shared hosting there are several websites hosted on the same server as you, so you don't know what the companies are or what their traffic is like. However, their activities could have an impact on your website performance.

With a dedicated server or virtual dedicated server, you have resources allocated to you. This means if you have reduced performance, you know it's because of something connected to your own website or server, so it's easier to resolve an issue. Our websites are on a dedicated server, so if there are issues, we know they are a result of one of the sites, which means we can isolate the problem and resolve it.

WHAT IS WEBSITE HOSTING BEST PRACTICE?

Your website hosting doesn't need to be in the same place as your domain name hosting. In fact, it's better that your website is hosted by a professional who can run backups, updates and monitor security. For this reason, it's not recommended that you try and host it yourself. Unlike domain names, where you get the same thing no matter how much you pay, hosting can differ widely depending on your service provider. This means cheap website hosting can mean a slow, unresponsive site and increased website down time.

When you do commission a website from a website designer, ask about the website hosting, whether the designer proposes to host the website after the site goes live and if so what they do to maintain sites and what happens if the site goes down or you want an update. This is often a weak spot for website designers and I've logged into a fair amount of websites running out of date versions of WordPress, PHP with warnings left right and centre and no backups.

WEBSITE BACKUPS AND UPDATES

WHAT ARE BACKUPS AND UPDATES?

A website backup involves saving a version of a website so that it can be restored if anything goes wrong. If you take and keep enough backups, you'll always have a stable version of a website to revert to if needed. With a content management system like WordPress, a backup will usually involve all of the website files and any associated databases.

If you have a website that is built using html only, then you won't need to run many updates, but most sites are now database-driven rather than a series of html pages. This means at the very least they'll need to update their PHP language to the safest version, which can occasionally have negative side effects. With systems like WordPress, there are constant updates being released of WordPress software itself and its themes and plugins. These updates are usually to add improved features, fix bugs and increase security. However, things can go wrong, with the worst-case scenario being your website going down. So, it can be tempting to avoid updates for fear of the unknown. However, over time that can also lead to your site breaking while also making it easier for hackers to target you.

WHAT ARE WEBSITE BACKUP AND UPDATE BEST PRACTICES?

We recommend running at least weekly backups, preferably from your hosting account. While content management systems like WordPress offer backup plugins, if your site goes down, you can't gain access to restore the backup. Having a backup system via your hosting provider means your site can be restored more easily and you can be more confident running all available updates.

Set your update schedule to run after your backups, so that you minimise the amount of data that might be lost if you do need to restore. For instance, if your backups run on a Sunday night, you then make changes to your site from Monday to Wednesday and then run all your updates on a Thursday but have to restore the website because of a conflict with some updates, you'll lose all of the updates you made between Sunday and Thursday.

Also, make sure that your backup retention schedule keeps copies of your backups going back a few months. This is because if your website gets hacked it's normal for the virus to sit dormant for a while before doing anything. This gives it a chance to infiltrate all of your backups and leave you without a clean and stable backup to revert to.

SECURITY AND SECURITY CERTIFICATES

WHAT ARE WEBSITE SECURITY CERTIFICATES AND WEBSITE SECURITY?

If you don't have a security certificate on your website, to many people that means you don't have a website at all. That's because when they try and visit your site, their browser will warn them against going further because your site is deemed unsafe, so many won't take the risk. Even if you have a security certificate, it may not be applied correctly with what's known as 'mix content', which is when some images use your security certificate and some don't. This usually happens when a security certificate has been applied to a site but the site content and links haven't been updated properly. Search engines like Google will penalise your site in search engine rankings for not having good enough security in place. However, once this is set up you shouldn't need to do anything to keep it working.

As we covered in the section about backups, websites can be hacked and you may not know that a hack has happened until your site is taken over or taken down. However, steps can be taken to make it harder to hack your site and for it to be easier and quicker to discover if you are hacked.

WHAT ARE WEBSITE SECURITY BEST PRACTICES?

Visit your website in a different browser or in incognito mode to see how it looks to other people visiting it for the first time, as this is more likely to show you any error messages. You can also look for the padlock at the beginning of your website address, which indicates that your security certificate is working. You can click on the padlock for additional information about the connection and for any warning messages.

Website hackers usually leverage weaknesses in website software. Plugins like WPMU Defender and WordFence give you a list of these and help you take action to close these loopholes. They also allow you to run regular scans of your site and report any suspect files and changes via a regular report so you can investigate. This enables you to spot issues sooner than you might have done otherwise.

If you've got any questions or queries about any of these topics, please get in touch to discuss them with us. We're proud of our proven track record in website hosting and maintenance, so if you feel it's time for a change, we can help with that too.

EMAILS

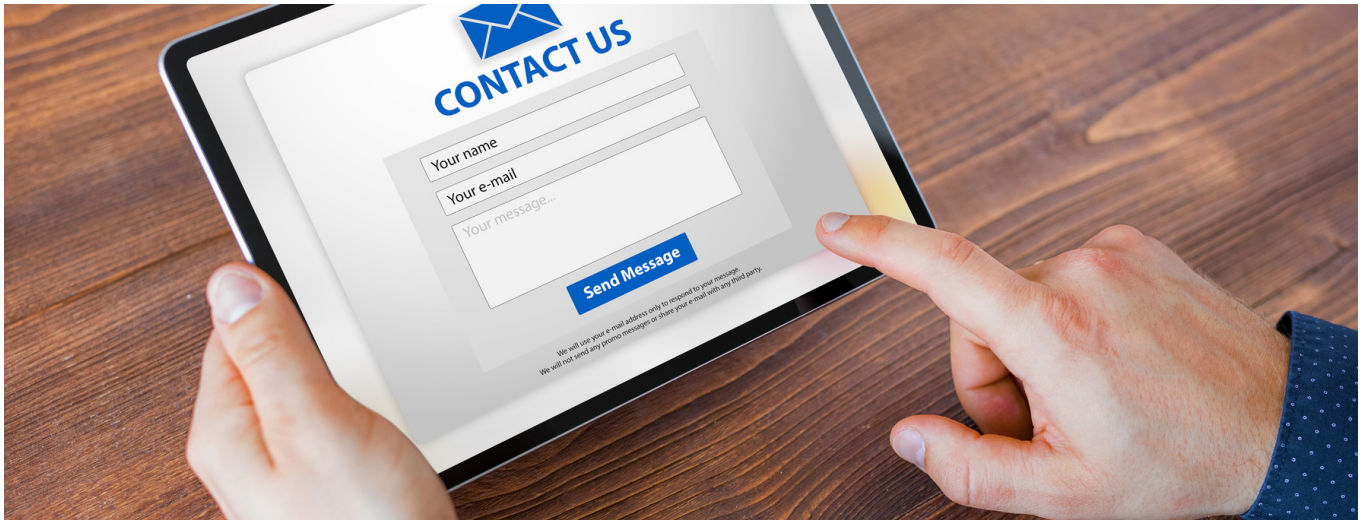
It used to be that the email addresses you use in the day-to-day running of your company were organised by your website company, but I don't recommend this unless they also specialise in IT. Previously emails were cheap and cheerful and often came free with your domain name. However, times have changed and these days your email is often the backbone of your company's operations.

While your website is an important asset for your company, if it goes down you can continue to operate unless your entire business IS your website, like an ecommerce or bookings company – I have a feeling Amazon and Air BnB aren't reading this PDF (would love to know if you are though!). On the other hand, If your email stops working, this means operations grinding to a standstill for many companies.

WHAT IS EMAIL BEST PRACTICE?

If you haven't already moved over to a professional email system like Microsoft Office 365, I recommend you prioritise this. You could get an email system from your domain name provider, but if you have more than a couple of team members, having support is worth its weight in gold in terms of mitigating the risk of the impact of email downtime.

WEBSITE EMAIL AND CONTACT FORMS



ISSUES WITH WEBSITE EMAIL AND CONTACT FORMS

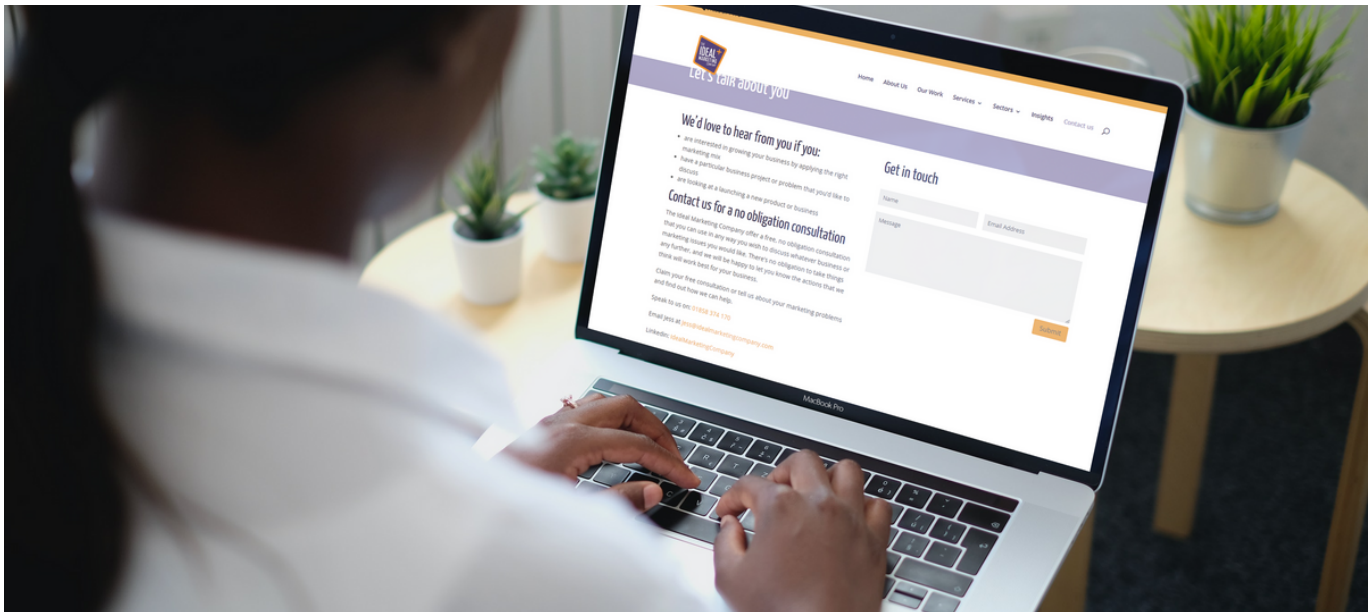
Contact forms on websites are a given, but what happens when someone fills in a form? An email should be generated from the back end of your website and sent to a predefined email address. Even if you don't have forms, there are many plugins on your site which need to send out email notifications, whether it's a security plugin alerting someone to an issue, or a broken link checker that's found a new issue. However, depending on the website hosting you have and your email filters, when someone fills in a form on your site the email may never be sent or arrive.

There are two main reasons why you might not receive an email sent via a contact form:

1. The default email function in a content management system like WordPress is just not reliable enough, so emails don't always get sent from the website or received by your email.
2. Your email filters won't let the email in, sometimes because it's too similar to your own email address. For some cyber security services, an email from your contact form can look like it's coming from you, which can flag it as a potential threat.

WHAT IS WEBSITE EMAIL AND CONTACT FORMS BEST PRACTICE?

1. Regularly testing the forms on your website is a good idea, in addition to ensuring a log of all emails that a site tried to send is kept. This way, even if you don't receive the email, you can still retrieve it. There are WordPress plugins that will enable you to keep and in some cases export a list of emails sent from your site. Sometimes the function is included in the plugin we mention in the next point.
2. Plugins like Postman SMTP allow you to use a third party like SendGrid, an SMTP account, Mailgun or the Google Mail services. This means that you're not relying on the PHP code that is usually responsible for sending email from WordPress. You will need to jump through some hoops to get set up and the third party will need authentication, which is getting more complex as email security gets tighter and tighter. The alternative is to remove all forms from your site, and just list email addresses.
3. If possible, make your website email come from a different address, like website@ enquiries@ rather than the one you use to send email.



PRIVACY POLICIES AND COOKIE PERMISSIONS

The following information is relevant as of December 2022 with websites in the UK. We'll do our best to keep this information up-to-date, but it is not legal advice and you should also consult the Information Commissioner's Office (ICO) or your own legal representation.

This area can be very confusing for businesses to navigate, in part because regulations continue to change and responsibilities can feel unclear.

WHAT ARE PRIVACY POLICIES AND COOKIE POLICIES?

A privacy policy explains how you collect and process personal data collected, whether the data is on your site or gathered elsewhere in the course of your business. There is certain information you must provide about how you process data, according to UK GDPR and often this information is shared on an organisation's website with links pointing to the page from email signatures or internal paperwork.

A cookie policy lists the cookies served on your site, and the purposes they serve. This is something you will probably need help from your website developer to produce because they know or can find out what cookies are served on your site.

WHAT ARE PRIVACY POLICY AND WEBSITE COOKIE BEST PRACTICES?

Keep your privacy policy up to date

A privacy policy is a legal document that you are responsible for creating because your website developer doesn't know the details of how you collect and process data throughout your organisation, so they're not qualified to tell you how to create one. For guidance on the kind of information it should include visit this ICO source. You should also speak to your data protection officer or legal representative. Your website developer should be able to set up the page and link or make any edits. Keep this information up to date when changes are made to how you collect or process data.

The same applies to your cookie policy – if you add a new function to your website, there might be a new cookie to report, so keep that in mind as you make changes.

Register with the Information Commissioners Office (ICO)

Are you registered with the ICO? If you obtain or hold data, you should be, and the ICO provide a handy 5-minute assessment if you're unsure. Once registered, add your registration number to your website footer.

Ask for consent before serving cookies

While many websites have a privacy policy at the bottom of their website and may even have a cookie banner, do you ask for explicit consent before loading cookies on your website? To comply with the regulations governing cookies under the GDPR and the ePrivacy Directive, you must:

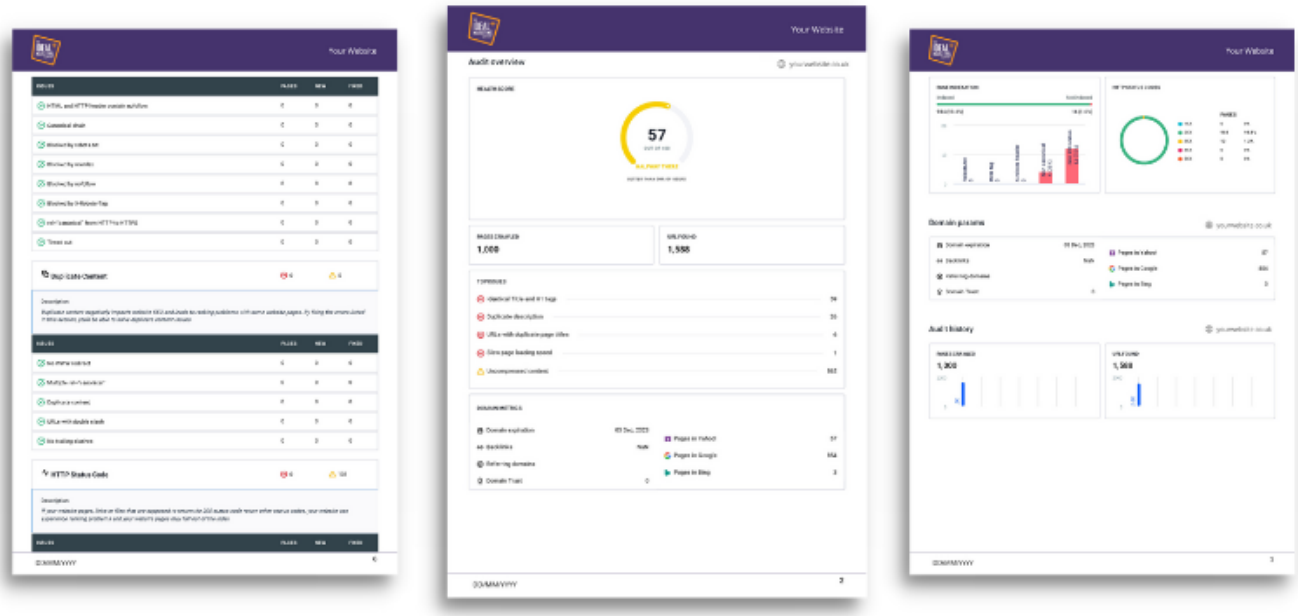
1. Receive users' consent before you use any cookies except strictly necessary cookies.
2. Provide accurate and specific information about the data each cookie tracks and its purpose in plain language before consent is received.

In a rush to comply with regulations in 2018, a lot of websites added banners that were available at the time, many of which don't require explicit consent before serving cookies, or state that the website uses cookies and if the visitor continues to use the website, they'll assume that's ok. Neither of these is explicit consent, so they aren't meeting GDPR/ePrivacy Directive regulations.

Unfortunately, the level of scripting required to stop cookies loading automatically means that if you're using WordPress, it can be hard to know which plugin to use. The CookieYes GDPR cookie consent plugin for WordPress gives you the option to scan for cookies, generate a cookie policy and load some cookies only after receiving consent.

WEBSITE SUPPORT FROM EXPERIENCED EXPERTS

If you've identified a few areas of concern and you'd like to talk it through with an experienced expert, get in touch. Also, in addition to our knowledge on these technical areas of website maintenance, we understand what makes a website into a business generating machine. To see how your website performs claim your free website review – you can even find out how your website compares to your competitors.



IDEAL MARKETING

YOUR WEBSITE CONFIDENCE CHECKLIST

DOMAIN NAMES

- [ ] Buy your own domain names or transfer existing domains into your account.
- [ ] Ensure your domain names renew by adding your bank account as a payment method, not just your debit or credit card.
- [ ] Buy variations of your domain name - particularly.co.uk and .com versions.
- [ ] Ensure that the email you use to login to your domain hosting account IS NOT an email address connected to your domain name.

WEBSITE HOSTING

- [ ] Ensure your website is hosted by a professional who can run backups, updates and monitor security.

WEBSITE BACKUPS

- [ ] Run at least weekly backups.
- [ ] Make sure that your backup retention schedule keeps copies of your backups going back a few months.

WEBSITE SECURITY

- [ ] Check if your website displays any error messages to users by visiting your website in a different browser or in incognito mode.
- [ ] Look for the padlock at the beginning of your website address to see if your security certificate is working.
- [ ] Identify weaknesses in your website software using security plugins.

WEBSITE NOTIFICATIONS AND COMPANY EMAILS

- [ ] Use a professional email system like Microsoft Office 365 that provides support when you need it.
- [ ] Regularly test the forms on your website.
- [ ] Use plugins like Postman SMTP to use a third party like SendGrid, an SMTP account, Mailgun or the Google Mail services.
- [ ] If possible, make your website email come from a different address, like website@ enquiries@ rather than the one you use to send email.

PRIVACY POLICIES AND COOKIE PERMISSIONS

- [ ] Keep your privacy policy up to date
- [ ] Register with the Information Commissioners Office (ICO)
- [ ] Ask for consent before serving cookies

CLAIM YOUR FREE WEBSITE REVIEW

www.Idealmarketingcompany.co.uk/get-a-free-website-review-report/

IDEAL MARKETING