WordPress Demystified Week 3

Security for Peace of Mind

We're week 3 of WordPress Demystified. I know, where's the time gone? Week 3 is security. So I said this is for peace of mind, but really it's also to protect your assets as well, because your website— hopefully you've grown used to me saying now— is a business asset, and so you really do want to protect that. We do that with the security.

So I'm going to start with something that is actually before you even get your website, and that is your hosting.

I know when businesses are starting out, it's easy enough to go for the cheapest available. And there are a lot of well-known hosts.

I'm not going to name names. Well-known hosts that are actually not particularly good. Just because a hosting is well known doesn't mean it's any good. So go and do some checking, and if your web developer has said, okay, we include web hosting in the design package, try and find out a bit more about that, see if they've had any reviews.

You can have the best website in the entire world, it can be beautiful, it can be fast, if it's on a really cheap, poor hosting, it's not going to perform And the likelihood is it's going to get hacked.

So part of the security, part of your peace of mind, is actually going with a really good quality hosting company. Now it doesn't mean that they have to cost the earth either. There are hosting companies like Venture IP, Prompt Web Hosting. Those are Australian hosting companies. They get back to you, they've got good support.

That's another thing you need to check if you're going for a web hosting company. What's their support like? You know, one of the reasons I recommend both Prompt Web Hosting and Venture IP, and I'm not affiliated with either of them by the way, is because when it comes to it and I've needed help, you know, a massive update has gone wrong.

I haven't had many clients get hacked, but if I have had, I need to know that the web hosting is there.

And on one occasion, like I said, I haven't had many clients. I think it's 3 in 18 years. One of those was due to a hosting company had not put up secure walls between the websites on their hosting. And when I was investigating how had the website been hacked, it'd actually been because another website had been hacked that had gone through then the hosting and come through to my client's website. So it wasn't the client's website, it was actually the hosting company they were using.

So security, we're going to start off with good hosting. Not necessarily the cheapest, not necessarily the most expensive, but good quality hosting.

Then when it comes to WordPress itself, when WordPress is first loaded on, there is a standard username called admin.

So one of the things I want you to do is to go and check on your website and see, do you still have a username called admin?

Because I'm hoping that if you've had the website built for you, they've removed that admin name and put something else there instead. If you built it yourself and you didn't know this, now is the time to go and use it. When you, what you want to do is create another, in fact, I'll put that in another video. I won't go into technicalities, but if you have an admin user, one of the things we wanna do is remove that and have something else at administrator level that is not called admin. Why?

Because hackers know that that's a standard default. And if they can find that on your website, It kind of means that other standard defaults may be in place as well. It highlights that you, although you're not vulnerable at the moment, you could have things that they could exploit.

Another thing, sticking with usernames and passwords, do you give out your username and passwords your administrator access to other people. I find this when clients, when new clients come to me and I'm saying, okay, I need a username and password, I need administrator access, and they'll go, oh, just take mine, use mine. And it's like, yeah, no.

If I have to, I will, but if I can show them how to set up A new username and password for me, that's easier for both of us. It's easier because they don't have to change their password after I've been in and used their account, which you should do, by the way, if you've lent it out to somebody else. You can't track who has done what on your website if more than one of you is using the same username.

There are plugins called Activity Log, and you can actually check who's doing what on your website, but that only works if you've got different usernames for different people. And the other thing is, if you stop working with somebody, you want to be able to remove them from your website. You don't want them to continue having access, especially If it didn't end amicably. If, you know, if somebody, a designer you didn't like, you want them off your website. You don't want them to go in for any other reason.

You know what I'm going to talk about with security? I'm going to talk about backups. Now, a backup is simply a copy of your website that stored somewhere else.

Ideally, you'd have several backups, and if you really want to be good, you'd have them stored in different places.

So you can have one stored on your hosting. There's— I was gonna say there's nothing wrong with that, as long as there's only one backup on your hosting. You also want backup on the cloud. Sorry, I think I've just been bitten by something. That's live, that's recording live for you.

So why more than one place?

You never know when something's going to happen to one of your backups or that it didn't even work properly. You don't know that, so you want to have more than one backup and you want to have it in more than one different place. You can have backups on your hosting, but not if that's the only place you've got them. And why I say that? Horror stories.

People coming to me and saying, I've lost my website because of a misunderstanding with a hosting company and it's all gone and I need a new one.

Because the hosting company is only going to hold your files for a certain period of time if they are not receiving payment or think that they are not receiving payment. This is why I like it, I like the backups to be stored in the cloud away from your hosting. True horror story, a few years ago in the UK, a hosting company was hacked and held to ransom. They ran the numbers and decided they couldn't pay the ransom. They emailed all their clients and said, we're really sorry, we hope you've got a backup elsewhere because we can't pay this, and so our business is closing down effective immediately.

And it was effective immediately because they couldn't get access to their own hosting. This was a hosting company in the UK. I don't know how many thousands of websites were affected by that. It's a horror story and it happened. Another story that ends happily is a past client of mine came to me and said, I know we haven't used you for a while, but you did our original website and we'd like you to recreate it because the hosting company We didn't receive the emails, we didn't pay the invoices because we didn't know we had to, and now the website is gone.

And she was saying, you know, so what's your current rates for creating a website? If you know what it used to look like, then that would be great.

And I said, so you haven't checked your Dropbox then?

And she said, Dropbox. I had set up a Dropbox account for her backups to go to. When she checked, there were backups from a few months beforehand, before they'd lost the website, so actually all we did was restore that on new hosting. They had their website back up and running, I think, within a day or two, and the They didn't have to pay me all the money to create a new website. So, so yeah, I did myself out of some funds that day, but I got the client up and running really quickly and they were happy, and actually so was I.

So this is why you back up to the cloud, okay? It doesn't matter if it's Google Drive, Dropbox, whatever you have handy, back up to the cloud.

So now that you have a backup and you're backing up to the cloud, the next thing I want you to do is, one, to have the settings on the backup so it's taking regular backups.

Now, how often depends on your website. If you have got an e-commerce website and you're taking orders every day, multiple orders every day, It may be that you want to have the backup every few hours because you don't want to lose too many orders if something awful happened and you had to restore from a previous backup.

If you haven't got an e-commerce site, or if you have and you're not taking orders that regularly, daily may be okay, weekly if you're really not taking that many orders. If you haven't got an e-commerce website, and you're only changing it maybe once a month, then back up once a month. But when you go to do the updates on your website, if you haven't hired somebody like me and my Web Care plans to look after your website for you, please take a backup before you do anything technical on your website and also before you make any big content changes on your website. Those are the 2 instances that you can take manual backups and it gives you peace. I only just thought of that.

Gives you peace of mind. Because if anything were to happen and you reach out to me and you say, Karen, you know, I don't know what I did with the website, something's gone horribly wrong. My first question is, did you take a backup? When was your last backup? Because if we can restore from there, I can get you up and running so quickly.

It's a benefit to you and it's a benefit to me. Stress less for both of us.

Moving away from backups, even though that's one of my favourite topics, you want to have a malware scanner on your website, again for security. Because in case those sneaky hackers have got in, sometimes it can be really obvious what they've done. It's like your website suddenly turns into a casino. You know something is wrong. You know hackers have been in there.

But sometimes it can be really devious so that they are maybe sending links away to somewhere else. So people will come on your website think it's completely fine, completely genuine, click on a link and go somewhere they weren't expecting.

This is why we have malware scanning, and I do that as part of my web care maintenance. I do that on a daily basis because you want to make sure that if they're in, you know as soon as possible. Because I hate to say this, but it is getting harder and harder to keep hackers out with AI and the way that they can use AI to get into websites

now. It is quite scary how relentless they will be, as in they can set up a programme. We've all If you haven't heard of bots, they're little programmes that will just keep attacking and attacking and attacking.

And this is why we have to be as secure as possible. And if they are in, we need to know as quickly as possible. We can get back, we can restore to when they weren't back in, or we can investigate how they got in and then restore. To before they got in and then fix the issue.

So we need to know if there are hackers there. Security as well is also your legal security, your legal documents. Do you have all your privacy policy, your terms and conditions for how you run your website, your cookie policies? Now I am not a legal expert, I'm not telling you to use one thing or the other. There is a company, they're a US company I think, Termageddon, they're the ones I use on my website.

They do the cookie policies as well and they are very good because you can tell, you can tell It's a massive tick here type forms that you fill in, and then they create the policies for you. If you are doing any business in the US, they go state by state because we think it's— oh, I think anyway it can be annoying here that there are differences between our Australian states. In the US, the changes are much, much bigger, and it goes down to legal requirements and policies and privacy and all sorts of things. So if you're dealing with actively seeking— this is actively seeking clients in the US, actively seeking clients in the EU— there are different laws there that govern all of that. Termageddon will handle that for you, and if you want to know more about that, let me know.

So you have to have wherever you get them from your legal documents, your cookie policies, your privacy policy. You may even want to think about an accessibility policy for accessibility for your website. I've spoken about security. But at the moment, for smaller businesses in Australia, we do not have legal requirements for accessibility. Bigger businesses do.

That doesn't mean though that you can't be accessible on your website. There are ways to check how accessible your website is, and this is from a point of view of fonts, Colours. So the look and feel. But why I'm mentioning that under security is because in

other countries people have been sued because their websites haven't been accessible enough. Besides which, if you believe in inclusion, then why wouldn't you want your website to be accessible?

Really, why, Would you not want people to easily read your website, for example, or to easily use your website? That comes under accessibility as well.

One thing, thinking about security, one thing that didn't used to be a big deal and now more recently is turning that way is hiding your WordPress version. So this actually always annoys me because I can go and have a look at the code on your page and see what WordPress version you're on. And it's like, oh, you need to update that. Oh, you don't, you're good.

It didn't used to matter too much whether you hid your WordPress version or not. Sometimes, most of the time, I would actually do that for a client. But it was out of habit more than it being a security issue anymore.

However, I was reading some security articles recently and what they are suggesting now is that it is a good idea to hide your WordPress version purely because of if you're on an older version of WordPress, when you update, when you're running the update for your WordPress core, it's the only time that your website, if you're on an older version, that your website has a, has a known URL. So most of the time When a hacker is trying to get into your website, they're having to use various different means. For older versions of website, when the update is being performed, just for those few seconds, the hacker can tell what your URL is going to be. So this is the web address when I'm saying URL, and if they can strike at just that time, they can get into your website. This was one of the big security holes that has been updated recently.

So whereas before I would have said it doesn't really matter whether you hide your WordPress version, now it kind of does, because if they come looking at your WordPress website and find out it's on an old version They're more likely to try and use these bots, AI bots as well, to try and keep hammering your website for just when you update it.

So hide your WordPress versions now.

Another thing about security, it's not so much if you have a standard website, but if you have an e-commerce website, you might want to consider using Cloudflare. Now what Cloudflare does is it gets rid of, it stops all these bots coming to your website.

So yes, it can be used for standard websites as well, but where it really earns its money is with e-commerce websites, and what can happen is that People who have stolen credit cards. So these aren't actually hackers, but these are people that have stolen credit card numbers and now they want to test them. It's actually called card testing. They will place hundreds and hundreds of orders on an e-commerce website to see what will work.

And I know this because I've had clients who have had this happen to them. Now the orders will fail, you will get hundreds and hundreds of failed orders unless they find a card that they can actually use. So they're normally targeting the cheapest thing on your website and they will keep trying it.

Now it's annoying, you can wake up thinking, oh, I've got a load of— oh, I've got too many orders.

With some payment companies, they may even charge because of all these failed orders.

I think that's more in the US than here, but I have heard it happening.

So getting Cloudflare is a— Cloudflare is a free account. Too many flus there. Cloudflare is a free account and you can hide your website behind it. It's changing DNS settings. I won't go into that here, but it's a really good way of protecting, especially if you've got an e-commerce website, and it's free.

You just have to know how to do some of the settings in the backend of Cloudflare, but that can protect you against people who would test card testing on your ecommerce website. So I know we've covered a whole range of things here.

Security is so important for your website. It does give you peace of mind for your business because your website is part of your credibility. If people go to your website and suddenly find casino on there, for example, they are going to wonder not just about your website but about your business and possibly even about you.

So we need to keep your website secure. We need to give you peace of mind. We need to give your clients peace of mind, your web visitors peace of mind, that they know who they're dealing with and that you're taking care of things. Even if that taking care of things is actually hiring somebody like me to take care of it for you. It means you care enough about your website.

I think we'll wrap up there. As always, there'll be more videos coming out during the week, smaller ones, bite-sized ones.

As usual, if you want to ask any questions, you can ask in the comments below. You can DM me on my Facebook page. You can email me, and if you're available Fridays, 10 o'clock South Australian time, that is, on my Facebook page, there will be a Facebook Live. Come along with your questions. They may be questions about security.

They may be questions we've covered in other weeks. They may be questions about something entirely different, as long as it's WordPress, that is. Bring your WordPress questions along. Every Friday, 10 o'clock South Australian time. And we'll see, maybe at the end of WordPress Demystified, if there's enough call for it, I'll keep doing that afterwards.

So this has been WordPress Demystified, week 3. I don't think I introduced myself, but you probably know. I'm Karen Leslie. I'm your WordPress Fairy Godmother. And what I want you to do, and what I want you to have, is a fantastic website that works for you and your business so that your light can shine out there because we need you.

There are people actively looking for your services, for your products, and we want to make sure they get to them as easily as possible.

So I want you to keep shining because we need you.

Until next time, keep shining. Bye.