WordPress Demystified Week 3 Live Q&A

Security and Peace of Mind

It's Karen Leslie, and this is WordPress Demystified, and we're actually on week 3, which, yeah, that is a bit of a surprise. It seems to have gone quickly for me. If you have, or if you want to say hi, if you're here, please put that in the comments. If you have any questions, please ask that in the comments as well. So this week has been all about security and peace of mind.

And I think that's becoming more important. I know for myself, when I'm looking at my emails that come through— so I have emails that are monitoring my WebCare clients' websites. I have emails come through to me on WordPress people and organisations that I follow so that I'm kept up to date with what's going on out there. And so much is changing because of the use of AI. So I'm not talking about people just going in and using Claude or ChatGPT or Gemini or, or whatever flavour of AI they're using.

I'm talking about the way it's being used. Just this morning I was reading about now when, when there's a vulnerability found in either like WordPress or PHP or a plugin, what some people are doing is trying to work out using AI how that vulnerability was found and how they can find other ones, or how they can see what code is changed and work it backwards to see how they can find other vulnerabilities. And this is beyond just trying to find ways to hack into the website with AI. So there's a lot going on around security. Security and peace of mind.

Because we do— we could— I'm not going to say we do— we could feel happy about our websites. We could feel secure with our websites. That's what I want my clients to feel like when they're on a Web Care Plan. So I do understand if you don't feel that way. I do understand that there are lots of changes going on at the moment.

It, it seems that rarely a week goes by when there isn't an update to something that needs to be done. So I get it, I really do.

So one of my— it was kind of a question— is how would I know if something's gone wrong?

So this was kind of talking about hacking, but also if something's just not working on their website.

So the issue with any kind of hacking is that there's, there's different kinds. There can be the blatantly obvious, so One past client, she came back to me saying, I'm getting some weird emails from my website. They appear to be in Chinese. Can you take a look for me? I'm away at the moment.

And when I looked, her entire website had been taken over by a casino.

There was nothing subtle about it, you know, flashing lights, the whole works. She had definitely been hacked. That's the really obvious hack. Then there's the more subtle hacks where everything looks okay, but when you click on a link to go somewhere, it redirects you to somewhere else.

So there are so many different ways that a hack Or be very subtle that you don't even know it's there, that it's really difficult to say, how would I know if something's gone wrong? This is why I have monitoring services as part of web care plans. Now, these are there for the developers. They're not really there for the general public. Because even if the general public signed up for one of these monitoring services, unless you're really techie, you're actually not going to understand what they're telling you anyway.

So I have monitoring services, and, you know, Wordfence is one of them. It's— you can have the free plugin Wordfence, and what that does is it comes along and it compares the files that you've got on your website that were released from WordPress, and then it matches them up. And so it will soon know if there are lines of code in your current one that don't match the original one.

And that will send you, it will highlight it at the backend of your website and it will send you an email on it. And then it's, well, what kind of change is it? Sometimes plugin developers are a little naughty and they will change the version of a plugin, as in they change the text in the comments of the plugin saying needs to have WordPress such and such onwards.

That's fine, but because that is different and they haven't pushed it through on a formal update yet from WordPress to WordPress, Wordfence would say, well, that's a mismatch. There's something going on here. So you actually need to go and then look at the code when you've got that warning message. So it gets quite complicated as to what is a change because of a hack or a change because a comment has been changed, for example. So there's all this monitoring that needs to be done.

You would probably only know on your own website if you're looking after it yourself when something obvious appears. Either it's stopping you from doing something or the links are being redirected.

You often don't have the level of monitoring on your normal website. Like I said, you can have Wordfence and that's free. You'd probably still have to contact me to let me know what's going on or forward the email to me and book a session, like a WTF session—WordPress Tweaks and Fixes, by the way, not what you were thinking. To see what that meant and how it could be fixed.

I used to be able to say that most of the time your website is fine, and and I and I can still say that, but I guess part of me is holding back from saying that now because I see the number of AI attacks that are going on.

And oh, I won't say it's relentless because that probably puts too much of a fear factor on it, but certainly some days and some weeks it does seem that there's one thing after another.

And it really doesn't matter what type of website you've got, they're still trying to get in. You may have a one-page business card type of a website and they're still trying to get in there, which I know is annoying and frustrating.

With the, how would I know if something's gone wrong after an update? So that we're taking hacking away now. After an update is testing. If you update a plugin that's for your contact form, test your contact form. If you've updated a plugin that does whatever the particular function is, say it's an online shop and you're using WooCommerce, then put a cheap— have a, like, a dummy product in there.

Set up a dummy product, set it for a very low price, and test it through the system.

The only way to know after a plugin is, is whether it's still working after an update is to test it. There is no magical way of doing things. There are automatic testing systems. Again, these are more aimed at developers and they can be quite expensive. So it's better that you get into a routine of if you're looking after this yourself, You're setting the time aside to look after this yourself, and you know what you're looking for.

You know what you're monitoring for.

Now again, I've got a— these are more, I guess, peace of mind things. What happens if an update breaks my website?

So I know it's easy to set websites up for automatic updates, really easy. You can, you can update absolutely everything automatically.

I don't like doing that. It's my perfectionist control freak coming out because you don't know when it's going to update. You're not setting a time to say, I want you to update at 2 o'clock in the morning because everybody's fast asleep and nobody's looking at my website.

There are tools that can do this. Again, they're not open to the general public, they're more developer tools. So the issue is that you can update your website automatically, and then if it goes wrong, you may not even know So although the question says, what happens if an update breaks it? Well, it's actually a step back that if you're doing automatic web updates, how often are you checking?

So I received an email from a past Webcare client. She's no longer a Webcare client, probably left about a couple of years ago, and she said, my website's gone down, it's got this really weird error. And it did, it had a critical error written across it. Oh no.

When I went and looked, she hadn't removed me from her system. So when I went and looked at all the logs, her website had been down showing critical error for 6 weeks.

So during those 6 weeks, anybody who have land— who has landed on her website has seen critical error. There is no way to contact her because all it says is critical error and an error code.

There's no way to contact her.

With me, I would be thinking about, well, how often are they looking at their website? Are they actually maintaining it at all? Do they know that this has happened? Why haven't they fixed it? Have they been hacked?

You know, all these different things. And it's really hitting to her, to me, it really hits towards their credibility. It's like, and there's no way of knowing if you're a web visitor, whether this has happened right in the last few minutes, whether it's been there for years. It may be something that you really want. So you may come back again, hoping that it'd be fixed.

And if it's not, then that's really denting The business's credibility.

So yeah, her website had been down like this for 6 weeks. She has no automatic monitoring. She has no— she has no system to go and check her website.

So what can happen, and what had happened in this case, is things are out of step.

So some things have updated, some things haven't. It's clashed. It's a big error.

Now I don't know what caused her to look at her website, whether she was about to do an update, as in a content update, or whether it was just she looks at it every 2 months. But it had been down for 6 weeks. I can't imagine, and I can't imagine in my business, just thinking of my business website, of not knowing what's going on with it.

I'm really aware that my business website is a business asset.

People go there. They check me out. You know, I may be well known in some Facebook groups, but they're still going to check me out. And I do that with other people. Oh, I like this.

What's the look? Oh, I like this. I go through and view their full profile. I am very disappointed if their full profile hasn't got their business email, business address visible, their website address, that is. I don't mind that they've got all their friends and their posts hidden.

I expect that, but I do want the business side there so I can go and check them out. And I will, I'll go and check out their website and see what they're up to. And does that match their socials, which goes back to alignment in that we did in WordPress Demystified Week 1.

If you're looking after this yourself, please put some system in place So that you know once a week you're going in, you're gonna take a backup, update everything, and check it's all working.

I, I ran a webinar a few years ago now about how to maintain your WordPress website properly, properly, but how I would maintain it, and these are all the different steps. And I taught this webinar and it was a free webinar. And to my surprise, some people's reaction was, really, you do all that? Yeah, I'll just sign up. This wasn't even— I hadn't even done a sales pitch at the end of it.

This was like a public service, if you like, a free webinar. And once people realised what was really involved, they actually signed up for Webcare.

So the security and peace of mind— the peace of mind is also if something goes wrong. If you're looking after your website on your own and something goes wrong, knowing who to turn to.

Even if it's like, you know what, I'm going to look after all of this, I've got the time, I've got my processes, I know what I'm doing, or I've got a VA that does it for me, it's still who to turn to when something goes wrong.

That's important too, because you do want peace of mind.

Yeah, going back to continuing with peace of mind, I don't know how often a website needs to be checked.

Oh, it's kind of, yeah, the how long is a piece of string.

So on my web care plans, I update clients' websites weekly. I have like a weekly rota that I do, weekly system. However, because I have emails coming to me to talk about vulnerabilities or plugins that, you know, you have to update immediately, I'm finding that I'm actually updating my clients' websites more frequently than once. If that comes

through, if these emails come through and it's like, yeah, okay, this is— so for developers, the emails that we get through will actually say things like it's a high vulnerability, which means it, it could be out there. People could be attacking other people's websites using that vulnerability in a plugin, that door, if you like, that they can get in.

Like leaving a backdoor. Literally a back door of your house open. That's what's happened, and people can get in and change your website.

So, sorry, I've just come up with that analogy and it has completely thrown me.

But we were talking about how often does your website need to be checked?

Weekly?

I would say weekly at a minimum. If you can get into the habit of even— if you've got like a business as usual or business as unusual, your daily list of things to do, if one of those can just be look at the back end of my website, does anything need to be done? Because if nothing needs to be, if there's nothing there, if there's no Updates or anything, fine, you keep going. It's just a really quick look at your dashboard. Does anything need to be done?

No, move on.

And if it's a yes, okay, what updates need to be done?

And go from there. But weekly at a minimum.

I think somebody heard me talk about abandoned plugins. So it's like, how, how do you know when a plugin's abandoned?

Which is a really good question. I use Wordfence. Wordfence puts in anything, any plugin that hasn't been updated within 2 years, it will mark as abandoned.

If you are choosing a plugin for your website rather than using a designer or a developer, It's one of the things I would always look at. If you're going to like the WordPress directory and you're looking for a plugin, just check the last time it was

updated. And certainly if you're using AI to recommend things to you, still check them. I was looking for plugins for a particular service that I'm not familiar with, and I wanted AI to give me a list. And the top one that it recommended, I went and checked it and it hasn't been updated in 4 years.

And I went back to AI and I said, so why did you put that as number 1 when it hasn't been updated for 4 years?

And it comes back with the good catch type of thing or my bad. However, that it's like, oh yeah.

However, if somebody didn't have the knowledge to go and check that first, they would have loaded that plugin to their website. And it would already have been abandoned. Now, what an abandoned plugin means is the developer hasn't updated it recently. It hasn't— they haven't checked for any security issues recently.

So part of this can be is that developers had different standards back 4 years ago than they do today.

So it's insecure if you put it on your website. An abandoned plugin can be insecure from the moment that you load it.

If you're looking, if you're looking for a plugin to help you on your website, book a call, get in contact, drop me an email, drop me a DM. Let's just go through some steps so that you're clear on what you're getting.

Being locked out of your website.

Now, I didn't get much else from this.

Ideally, when you have your WordPress website handed over to you, you would have an administrator username which can do everything in the universe, and you'd get like an editor username who will just deal with the content. So the editor one is if you know you're just going to put a blog on there, that can be really useful because it allows you to go and put the blog, your content on your website without the ability to do anything else.

When you have your website given over to you, there's normally the admin of the web designer or web developer who created it for you, and if you're still in touch with them, that's fine to leave it. I would suggest creating another administrator user profile with another email address.

So if you have 2 email addresses, use another one for that admin. You can't use the same email address. The reason that can be useful is because if you lose access to one email address, then you've got the other one, because I'm not quite sure what When they say being locked out, you can always reset your password and that will email you a reset link to your existing email address. However, if you've lost contact with that email address, having 2 email addresses as admins on your website can be useful then, so that hopefully you don't lose access to both email accounts.

Whoa, which updates are safe?

I'm sitting with that because I'm actually not sure how to answer it.

You kind of You can, you can go on the assumption that all updates are safe.

In that, you would still take a full backup of your website, send it to the cloud, and then do your updates.

And it depends on what you're updating, I think, also is the, is the Which updates are safe?

If it's— so you can have major releases from WordPress, or you can have— and you can have minor releases, and you can have security releases. Now, a big release tends to be when it moves from like 7.4 to 7.5. That can be a major release. If it goes from a 7 to an 8, that can be a major release. Not that we're there yet.

And what I would do, so what I do with my clients, it's like, great, there's a new major WordPress release out.

It's not a security release. So it's not something we have to update immediately. They may tell you otherwise, but if it's not a security release, you don't have to update immediately. And what I tend to do is I sit back and I wait until other people have updated their clients' websites or their own websites to that latest big WordPress

release, and then I see what happens. And I tend to leave it at least a week And in that time, obviously, I'm in different groups that will— if it's gone wrong, I'll know fairly quickly because there'll be complaints and whinging going on in some of the forums.

But also you can then do a search in a search engine and say WordPress, whatever that version is, issues or problems, and see what it comes back with. Because WordPress is now this massive system, and although they test it, they give it some really thorough testing before releasing it to the public, that doesn't mean that it will necessarily work immaculately on your website. It could be that a plugin or a theme doesn't connect well with it. And so it may look— the website may look a little bit stranger or strange than it did before.

It could cause an error. It could slow the website down.

But for me, I will always wait until somebody else— when it's a major release, until other people have updated it first. Let them deal with any issues, and then I know. Especially if it's an e-commerce website, I tend to email out my e-commerce Webcare clients and let them know, yeah, I'm aware the latest version of WordPress has come out. It's a major release. I want to be able to test it on your web— your website, on the demo or staging website.

That they have. I want to test it on there first before I put anything live, and I want to see what other people are coming up with issues. So yeah, but do, do a backup first, a complete backup. Send it to the cloud, send it to multiple places if you want to, but usually the updates are safe. It's not like they come with a warning, but if you're— if it's a major WordPress one that, that you are doing yourself, then wait until others have done it first, or come to somebody— not somebody like me— come to me and say, Karen, can I book a WTF session for 30 minutes and let's go through And update the website.

We can do that.

How much access to give?

I can't remember if I've loaded up this bonus video. I will go and check after this. I've actually done a video in how to create an admin user. So when you come to me and

you say, Karen, I'd really like you to look at the backend of this, or I need this updated. Rather than say— rather than email me with your username and password, uh-uh.

What you can do is set me up with my own username and password that will be emailed to me.

That means your username and password is still safe. Because the more people you share your username and password with, The riskier it becomes because it's out there. And if you have a VA working on your website, they should have their own username and password. They should not— sorry, that was an alarm on my phone going off. They should not be using yours for security and other reasons.

So there, there are lots of things you can do for security and peace of mind. I haven't even talked about Cloudflare, and Cloudflare— put my teeth in— is a— there is a free tier on that that you can get rid of some of the bots and the AI stuff that's attacking your website. There's a free version of that that can do that. You still have to know how to set up all the rules. It's built for developers, not for normal human beings.

Sorry, developers, it's not made for that. So there are rules and different setups, and if you use Cloudflare, you've got to use— what Cloudflare does is it's the in-between the web visitor and your website. So if your website's over here, your web visitor's over here, this is Cloudflare in the middle, and the web visitor will come through and it's like they have to get through Cloudflare first. You may have even seen the tick a box if you're human. Cloudflare is used by lots of massive companies.

But it's actually available to everybody. You just need to know how to set it up.

And yes, I do know how to set it up, in case you were wondering.

But the, the, the best way really for peace of mind is to take regular automated backups and send them away to your cloud hosting, your cloud storage. It really is. When something is wrong with your website, it's one of the first questions I ask, because if your website has been hacked, it can be because updates have not been done for a long time, like a very long time sometimes.

So I will always ask about a backup. Sometimes what we can do is restore from the backup, do the updates, and your, your website is clean. On other occasions, you need

professional— other professionals to come in and actually clean your website. It's not, it's not a speciality of mine. There are services that you can use that will clean it up.

The last time I looked, it's about $280 Australian dollars.

There will be a service that I'm going to be using with my Web Care clients. They don't know this yet, by the way. Uh, That it will be about half that price. If, if the website was hacked on the new service that I'm going to be introducing to my web care clients, then it will be a lot cheaper for them to get it cleaned. So that's something that they don't know about yet, and now you do.

So when things are coming out, I'm always trying to improve my web care plans. Improve the security, improve the peace of mind.

Because you're worried about your one website, maybe you've got more than one business, but you're worried about your one website. I'm worried about all my clients' websites, and I want to make sure that I know what's going on out there in the industry. That I can improve or add to my services to keep them secure and give them peace of mind.

Now, I haven't seen any questions in the comments. I will come back and check later, or it will notify me later. I hope that's been useful. A recording of this and the transcript will go on to the WordPress Demystified resources page. If you haven't signed up, it's like, what have you been doing?

If you haven't signed up for WordPress Demystified— I am joking, by the way. If you want to sign up to WordPress Demystified, you get all the resources over 4 weeks. I release them each week. You get checklists, you get transcripts, you get bonus videos. You know, if people— if I get enough come through of the same question, I may do a video to explain that.

So this is evolving. WordPress Demystified is evolving, and it's completely free.

So if you want recordings, transcripts, checklists, bonus videos, I'll put the link in for WordPress Demystified so you can register. It's free.

There are no more questions I've got. I can't see any more in the comments, so I'll wrap up this live.

If you're here with me live and I haven't seen your comment, I apologise. I'll go and check now. Thank you for joining me. If you're watching the recording, Thank you for joining me, and ask any questions. And if they're questions that you think, oh, it's too dumb to ask that question, I can guarantee somebody else is thinking of it, and they may be thinking it's too dumb as well.

If you don't want to put it in a comment, if it feels— if it feels hard to put it in the comment for whatever reason, DM me. And I can answer you through DMs. It's not a problem.

This is Karen Leslie. I'm your WordPress Fairy Godmother. That was the Q&A, live Q&A for week 3. Next week, it's going to be about WebCal. I know I've talked a lot about it this, this session as well, but WebCal and your business sustainability.

Hmm, it's juicier than it sounds. I know people think, oh, maintenance, web care, boring.

Your website is a business asset. Like I told you, that client that came back to me, she didn't know it was down for 6 weeks.

6 weeks. Just saying, critical error, no way to contact her.

I don't want that happening to people.

I really don't. So next week it'll be about web cow and business sustainability, because to me they're hand in hand. If you have any questions, even for that topic or any others, you can either put them on a Q&A live and I'll pick them up from there, or DM me or email me if you have my email address. But that's for next week.

Until then, I hope you have a fantastic week. I hope you take up space. I hope you shine your light because that's what websites are about. They're helping you shine your light into the world.

Keep shining.