myweeklymarketing.

Episode 9

Is Your Online Business Secure? with Lori Martin

Janice Hostager: And then transcribing at the same time, perfect. Well, hey there Lori. How are you today?
Lori Martin: I am doing great. It's kind of a rainy day, but everything's good here. So, so happy to be here and…
Janice Hostager: We love that in Texas.
Lori Martin: excited to be part of your Podcast. So thank you for inviting me.
01:17
Janice Hostager: So tell me about your business and what you do.

Lori Martin: So, I started Double Fox websites in 2008, and I first got into the Internet space back in the mid-90s. When it wasn't even a space, I was just doing kind of, what we would call the first SEO for businesses. I worked for Garden.com and Digital Cheetah and then I found my place which was just trying to help people. In a small business community leveraged, their leverage the online community just be able to do those things.

02:03
Janice Hostager: And SEO for anybody that does not know is search engine optimization because we build websites. Not just for customers, but also for the search engines, right? Is that right, all right.
Lori Martin: Yes, yes, so yeah. So when I first started doing it was the very earliest part of SEO And I got these businesses online at Yahoo listings, and these different listings that people don't even know about anymore. But Now, I am moving to small businesses.
Janice Hostager: That's awesome.
02:39
Janice Hostager: Okay, so now you have a website company that builds fabulous websites, but you have a passion for security because obviously in this day and age, security is a big deal with a website with everything online, right? So,…
02:55
Lori Martin: Well, I became passionate about security and early on when I got so many websites so much business that had been breached and breached in a traumatic way so that they wouldn't like Google actually blacklisted them.
Lori Martin: What are the ones that were really eye-opening and I'm just going to say I'm a WordPress girl. So I'm just all about WordPress, that's what I do. I build and WordPress zones

about 40% of the market share and in content management systems. Meaning that if you have a website, you're going to use some sort of platform and WordPress is open source and one of the biggest ones out there. So, when I talk about,…
Janice Hostager: Right.
Lori Martin: The things I talk about, it's going to be primarily WordPress, even though I've been involved with Drupal and Weebly, and Wix and Square. I'm always going to talk about WordPress. So you one of the things that really was I opening for me that really got me into the security area was I was working with the contractor. And this contractor, their manager sent me emails, very good communications, beautiful contractor. But when I would eat, when I would click on the link in their email, you would always send me to a pharmaceutical company.
Janice Hostager: Hmm.
Lori Martin: And so I was, I said to them. Well, can you send me an email? Just send me the link to your website so I can see that I just want to see you know, what's going on like what? Before and after some of your projects, some of your work but she said, well, it's there in the email And then it became obvious that they had been breached, they had been hacked, and so, if you were an admin user, or if you were looking on Google, you would see their website. But if you looked anywhere else, you would get this pharmaceutical company. So this was a very advanced breach that I was very shocked about but it was very opening.
05:08
Janice Hostager: Hmm.
Lori Martin:. So that's when I really got into it.
Janice Hostager: Right.
05:21
Janice Hostager: So when I created my first WordPress site, I installed a plugin that allowed me to get an email whenever someone tried to hack my site. And I thought it would be kind of interesting to see. Oh, if someone tried to hack my site today, what I wasn't ready for was that I started getting emails about attempted brute force hacks about every hour or more. I mean it was constant just over and over and over again. and I was really blown away. It's brute force is that which is where people just try and figure out your password and try and log in pretending to be you. Do you know if that's the most common type of vulnerability? Or when do most websites, or how do most website vulnerabilities happen?
06:07
Lori Martin: Well, there are several ways and I just wanted to talk about passwords because I have an analogy. I like using analogies because I think people can see them. But you picture your big castle and you have got your hundred foot stone. Walls around you and you have got a moat around you and have got a drawbridge, you've got security around you. And then little of me walks up on my donkey and has the right password and the drawbit bridge goes down and I just entered. So passwords are a really big deal and they are what you were talking about your brute force attack and stuff.
Lori Martin: These are the things that the servers are going to be trying to do and they're not like they're robots, they're not humans doing this stuff. So your password, if you think about your password, if you have another analogy, if you have a password of one character, and let's limit it to just some numbers. You've got zero through nine that's 10. You've got 10 digits and a person could hack that in no time as could a computer or if you turn that into two digits. Two areas

even, we're just limiting to numbers, you've got 10 times, 10, you're going to remove some of the duplicates.
Lori Martin: So let's say you've got 90 and then every time you add another value, it becomes harder. And so I looked into this and so remembered. So if you look at your keyboard you have 10 numbers and 52 letters because we're talking about lowering uppercase and maybe like approximately 32 different characters. So those are all spaces that you can use. And so, a 12 character string is estimated to be taking 7.5 million years to figure out.
Janice Hostager: Wow. Wow. So, so
08:34
Lori Martin: Right? Seven characters is about nine minutes. Most people don't think about that. But there's also the computer, the server, the hacker is going to be looking at common passwords. There's published common passwords out there and the first thing they're going to do is look at those common passwords and…
Janice Hostager: Hmm.
Lori Martin: they're also going to look at things that are associated with you. Such as your name, your username, your company name, your dog's name, anything out there. That's how it becomes. That's how they can break it down because you think If a 12 character string takes 7.5 million years, that's not going to happen unless they know something about you. So your passwords are so important. Like I said, me walking on my donkey up to your castle that has all the fortification possible. I'm walking up and if I have the password, I'm getting in.
09:46
Janice Hostager: Right. Right. So that's like the weak. The weakest link basically is that is your password.
Lori Martin: But we sure, I mean, obviously your website has to have the security in place, but that's the first place people are going and when you say brute force attacks and those kinds of things they're going after your password. And so, you just want to make sure that you have a very strong password and don't really use your password. I use a password vendor, and there's like, there's plenty out there, I use robo form. There's What what? There's a bunch of them now they're all…
Janice Hostager: Like, like Lastpass or some of the others.
Lori Martin: But the good thing about using them is that when you know your password is breached, you can also search in your forms, what password was breached and you can change all of those if you're still using the same password, you can change it. And I learn now that I don't even use the same password ever. But if you're using the same password, then you know which sites you need to change.
10:55
Janice Hostager: So, what you're saying is if somebody wanted to break into my website or hack my website. All they would have to do is basically maybe go on social media and find out a little bit about what I, where I live. Maybe so you're saying that even if I have pictures of my dog or my kids or anything, where I include names that they're going to maybe try those if they wanted to. They really wanted to break in. What about things like phone numbers and zip codes. I mean, all of those things kind of leave you two vulnerable, you think?
Lori Martin: All of them, all of them. Like, it's, you know, and they're and, you know, these guys like the hackers are not going after you personally. For the most part and unless you're an

Amazon or something, but they're, you know, they could go after you and find this information and you may be breach and you don't even know it. They're just using your website, your server to do other stuff. I had one client come to me and her website was full of Arabic information. She looked at it every morning and saw just nothing but Arabic stuff. So…
12:13
Janice Hostager: So what else can we do with our websites? Okay, a strong password. That's number one. What else can we do with it? We'll say WordPress because you know, it is the most common one out there, although I'm sure some of these apply to other types of websites too, but what is your next recommendation?
Lori Martin: All right, so yeah, passwords are really really big. Don't send them over email and email is not encrypted for the most part. So when you, if you thought you would ever send your social security number in a plastic email or a plastic envelope. Don't, that's what you're doing. So don't send your Email, your passwords or anything like that. To separate them at least you…
Janice Hostager: Okay.
Lori Martin: your password name, your password email, if you have to do it but it's not encrypted. So keep that safe.
Janice Hostager: Better.
13:07
Lori Martin: Your domain name, make sure, you know where your domain name is registered. That's a big one and has a strong password that's associated with wherever your domain name is registered. Where is your domain name registered? Doesn't mean that's where your website is hosted. It just means that's where you've got your password, or your domain name listed.
Janice Hostager: So when you go to reserve your domain name, if it's like Godaddy.com or some of the many, many other sites out there. That's separate from where your website is actually hosted sometimes, sometimes it's not, sometimes it's the same.
13:45
Lori Martin: Yeah, absolutely. Absolutely. And there's a reason to have it separated, your domain name and your website, and your email, especially your email. You don't want to host your website because if your website goes down, so does your email, so those separate?
Janice Hostager: Oh right.
Lori Martin: But absolutely, no. We're just your domain name registered because that is the key to your website.
Janice Hostager: Okay.
14:14
Lori Martin: I've had clients come to me and say we can't move our website and somebody has control of the registration. And I can't do anything about it, because It's, you know, whoever registered it. So I don't like to register for my clients. I don't like to register their domain name, I will do that, but I always recommend that they have control over their domain name because that's the real key right there.
Janice Hostager: Number three. Is there number three?
14:53
Lori Martin: I want your website to be Serving up as HTTPS, which means you have an SSL certificate. SSL stands for Secure Socket Layer and it's just going to deliver the communication between somebody looking at your website and your website. It's going to be encrypted. So

when you as the website owner, when you log into your website, You're going to get your password information, that's all going to be encrypted. So it's safe and secure. And that's what you want.
Lori Martin: And anybody who adds information to a form or anything, it's all going to be secure. So you want to have that SSL? And what can happen is, you can have a SSL certificate but some of the possibly images on your website or other things. We're not added in secure form. And so what you'll see when you look at your website and you're going to look at the browser, the browser address and you look in the top left and you'll either see a log icon or you may see a big red string. No, not. Which means you don't have SSL security or you may see a little triangle there that says you're secure, but not totally secure. And that means that some of the items on your website were not added in SSL mode.
Janice Hostager: So how do you change something like that?
16:44
Lori Martin: And that depends on what it is, but what I've seen and this is just me what I've seen is, you can go into your media library and just add an s to the image. Like, there's different images.
Janice Hostager: Oh..
Lori Martin: You can add an s to the URL, but
Janice Hostager: So that would be images that are posted that are hosted on another site that you just are pulling in from another site. They're not uploaded to your side per se, correct?
17:19
Lori Martin: They were uploaded to your site but not insecure mode. So sometimes, it's as simple as just adding an S to and that's all I can speak to.
Janice Hostager: Okay.
Lori Martin: I can't tell you know, talk about all the other things, but that's a possibility. Yeah.
Janice Hostager: Sure. Okay.
17:39
Lori Martin: All right. Another big one is do not allow everybody to have admin access and I'm talking about WordPress. But whatever your website is, whenever you're using it, make sure that all of your users have their own login. And restrict who has access to the higher end. So in WordPress, admin means that people can add plugins, they can add code, they can totally destroy your site. So we restrict who has admin access completely but just make sure that you don't give everybody admin access.
Janice Hostager: Great advice and I think oftentimes will do that, right? If you have somebody that's helping you with something, you or…
Lori Martin: Yeah.
Janice Hostager: You might give them your own password? And and…
Lori Martin: Yeah, yes. Yes.
Janice Hostager: Just say, Oh, just log in under me, but you're saying that's not a good idea.
18:44
Lori Martin: It's not a good idea, because you want to be able to see in the logs who did what? and so…
18:51
Janice Hostager: Mm-hmm.

Lori Martin: If it's separated you can say, okay, this person did this. This person tried to update this, whatever it was. It's very important to have different logins and different access and admin access should only be top-level people that you want to be able to do things like in our company, we only allow admin access for our company and nobody else gets up in access because we don't want them to be adding plugins which will be our next conversation. And right,…
Janice Hostager: Yep.
Lori Martin: It's like there's a lot out there. There's so much to talk about. So I guess that brings us to the next question, you're going to ask.
19:44
Janice Hostager: Yes, it was about plugins. I mean,…
Lori Martin: Oh..
Janice Hostager: How do you know if you have a vulnerability and a plugin?
Lori Martin: Plugins are so let's say that and like I said I'm a WordPress girl but plugins are and they're written by you and me and all of us out there and some of them are supported and some of them are not, but they are, they can provide great functionality, but they're also vulnerable. So you just want to make sure that the plugins that are out there, are tested with WordPress and Woocommerce normally but they're not tested with thousands of plugins that are out there. So you can have, you can just think about kids on the playground and you add more and more and more and they're not all gonna get along.
Lori Martin: And that's what it is with plugins. They can be great with WordPress and with Woocommerce, but they may not get along with the other ones, so you get conflicts and vulnerability. So, yeah, you just have to be very careful and it's critical to keep your plugins and software up to date and as you mentioned, is it automatic or not? You just have to choose if you have, I wouldn't do anything automatic unless I felt it was secure. Sometimes what we normally do is,…
Janice Hostager: Okay.
Lori Martin: when we add a plug-in, or we update a plug-in, we wait for a few versions on anything like 4.1. 5.1. 3.1. Those are big, those are big ones but if you go a few versions over, they have got through the bugs so we don't typically add the plugins or update the plugins when they're first added.
21:58
Janice Hostager: Okay. Okay. Yeah, I was actually wondering about that because I think I was under the impression that if there was an update that it was important like it may be a security patch or something like that and I should be right on top of it. Updating that plug-in to make sure everything looks works for sure and maybe it says that in the update too like this is a security patch or this is just an update. So my thought was, well I click this box, then it’s an automatic update and seems like the most prudent thing to do. But you're saying maybe just check your site every so often to go through and see what plugins need updating and maybe just hold off and on some of those.
Lori Martin: Yeah, so there's definitely I've seen the security patches and updates and those are the ones that you definitely wanted to take care of right away. But the major changes, the major versions, so if you're going from a one to a two, two or three to a four. Those are ones you could probably hold off on a bit because they have a few more bugs.

23:08
Lori Martin: So normally if there is a version that goes from like a one point something to a two-point something, then that's a major.
Janice Hostager: Right. But let's say I need a plug-in for something on my site.
Lori Martin: What I normally do, when a client wants to see a plugin and add it, I look at the reviews. And I look at the updates and I look at how long it's been going. And then we can try it. If it's a really new plugin, I probably won't even try it.
Janice Hostager: Oh, really? Okay.
Lori Martin: Yeah, I mean you just don't know if it's going to be supported and specially the free plugins, you know here. You're using a free plugin, and whoever created it, it probably has a side job doing something else and…
Janice Hostager: Mm-hmm.
Lori Martin: It might not be supported in a year or two. So, Just think about that.
24:15
Janice Hostager: Okay, just kind of Google reviews and do your research before adding anything to your site.
Lori Martin: Yeah..
Janice Hostager: One thing I really hate is the recaptcha on forms, you know having to click those little pictures that have the bridge here or…
Lori Martin: Yes.
Janice Hostager: have the flags or whatever, you know. How important is it to have those on your forms? And is it more trouble than it's worth? Or what do you think?
24:38
Lori Martin: I would always have them. I know they're a pain but just like passwords are a pain and I have had clients who have had comments and guest books open that people can add things to their comments, their reviews, not published. but, It still fills up with spam immediately. I had one client that we had to shut it down and he had over 600 comments there. So it's very important to have that kind of a little bit of blockage so that even the spam boxes that are coming in, are not able to do it.
Janice Hostager:Gotcha. And about an actual set of eyes to do it.
Lori Martin: Yeah.
Janice Hostager: On most WordPress sites, you can log in by going to the URL slash Wp-admin. I, you know,…
Lori Martin: Yeah.
Janice Hostager: I happen to have worked on a site that you had done and I noticed that you changed yours. So is it bad to keep that there? Or is there a reason why you want to change that and how do we change it? How do we go about changing it?
Lori Martin: Well, it's just an extra level of security because you're right, everybody? Who knows WordPress knows that that's the first access trying to put in your password. So we added a plug-in that changes it. I can put that in my show notes, give it to you.
Janice Hostager: Perfect.
Lori Martin: Just an extra just one more level of security, that's all that was.
26:18

Lori Martin: The backups are so important and you want to back up your website but also a backup. Not only where your website is but also on a different server because if your server goes down, your backup goes down too.
Janice Hostager: Gotcha.
Lori Martin: We provide daily backups for added security in three different places that we have it on your website and then at your data center, and then someplace else a different data center, so I guess it really depends on your website. If you have a blog website that you're just doing, Once in a while, you know, you update it once a week or something, then your backups could be weekly or once a month but we do it daily because we have clients who are updating their website daily.
Janice Hostager: Sure. Okay. Anything else we should be worried about with our websites?
Lori Martin: There's always, there's always more but I'm just gonna leave it at that.