PLEASE NOTE: This is a machine transcription. Some punctuation and spelling weirdness are to be expected.

What if you woke up one day, sat down at your desk to get some work done. And you discovered that you couldn't access your website? Or your shopping cart? Or your membership site? Would you panic? When it happened to me, I didn't, at least not right away. But as that morning dragged on, and it became increasingly clear that my website, actually, you know, what, not even my website, but my entire business was offline, I became more and more concerned. I contacted my website hosting company, and I was told that we'd had a server crash, but they expected it to be back up and running within a few hours. Unfortunately, it took four days before we were finally back online. And after losing what I can only guess was about $4,000 in revenue, we regrouped and put new processes in place to ensure that never happens again. This is Episode 43, of the Tiny Course Empire Podcast. And today, I want to talk to you about protecting your business from this kind of disaster. Because honestly, that server crash could have put us out of business. And I don't want that to happen to you.

Hey, guys, it's Cindy from the Tiny Course Empire Podcast. As always, you will find show notes and recommended resources for this episode at TinyCourseEmpire.com/43. While you're there, I also have a disaster prevention and recovery checklist for you. That's going to help you make use of all of the tips that I'm going to give you in this episode. If you're new here, be sure to hit the Subscribe button, because you're not going to want to miss next week's episode where we're going to go a little bit lighter and talk about my favorite free tools. But that's next week. This week, we're talking about a hard subject. We are talking about all of the things that can and will at some point go wrong in your business, and how you can be prepared for them.

That story you heard in the intro really happened to me last summer. And if I'm honest, it was entirely my fault. I'd been running an online business for more than 10 years, and I'd gotten complacent. I trusted that things that we put into place were still working. Even though I had seen this type of disaster happen to other people. I'd even cleaned up client sites who had this exact issue. And I still didn't think it would happen to me. I thought we had adequate systems in place. And I bet you think the same thing too. But let me tell you, even if you do all of the right things, disaster can still strike.

We had good hosting, we had backups, it just wasn't enough. And disaster comes in lots of different forms, too. We happened to have a server crash. But it could have been a natural disaster that destroyed our home and all of our computers, it could have been an accident, like dropping my computer in the lake, I would never do that. But you know, it happens. Or it could have been something malicious, it could have been a hack on our website or on our shopping cart. There are all kinds of different things that can and do go wrong in online businesses every single day. But there are things you can do to prevent that from happening to you. So what should you be doing to prevent or at least minimize this kind of disaster in your business? Well, I have some tips for you today. So let's go ahead and get started.

First of all, and this is going to sound familiar, but back up your stuff. So many people don't do this. And it drives me crazy. Did I ever tell you guys that I used to work for a website security firm, I used to actually spend a part of my week cleaning up hacked websites. We would go in and manually sort through all of the WordPress files and find the malicious code that had been injected into the site that was causing all kinds of problems or maybe defacing the site and manually

cleaned it up. It's very labor-intensive job to do. I actually enjoyed doing it. It was a lot of fun for me, not so fun for the people whose sites had been hacked. But I will tell you this, if they had a good backup, it took about five minutes to do if they did not have a good backup. It could take anywhere from four to eight or 10, or 12 hours or even more. So keeping a good backup is the key and keep multiple redundant copies.

I said a minute ago that we had backups when our server crashed. But we didn't have enough. The backups that we did have were old, and we had to piece them back together, it took much more time than it should have taken us if we had had those multiple redundant copies. So what do I mean by that? When I say multiple copies, I mean that you should keep a copy on your server, we use Liquid Web, which has an off server daily backup that we can access easily enough through our account. And we also use Backup Buddy to keep a backup on our own server. We also keep backups in a cloud location. So for you, this might be Dropbox or Google Drive, or Amazon S3, we use Dropbox.

But and I want you to be careful with this. This is just an aside. But don't fall into the thinking that Dropbox is a backup because it is not. If a file is corrupted on your computer, it's corrupted everywhere. It's synced with Dropbox. So it's not a proper isolated, secure backup all by itself. A backup by itself is something that is on a drive somewhere else. So for example, even though my Dropbox files are synced with my laptop, and they're synced with my husband's laptop, and we have them in multiple places, they're also backed up on an external hard drive. I use a Seagate, two terabyte hard drive that's connected to my laptop, and it backs up through the magic of something called Time Machine on the Mac. So I don't ever have to think about it. You could also set up a service such as Backblaze, or Carbonite, I've used them in the past, and they have a really good service that just automatically keeps your computer backed up whenever you are connected to the internet.

Now, you might be thinking, this is overkill, Cindy, you've got, you know, six or eight copies of everything. But I will tell you what I would rather be safe than sorry. In this regard, I would rather have six copies of everything and never have to use them, than not have one copy when I really need it. So keep redundant multiple copies of your backup. And keep more than just the most recent backups in case you get hacked.

So what often happens, what people often do is they have a good backup system in place, they're backing up their computer or their websites. They're backing those up every single day. And they're keeping maybe a week's worth of backups. But what happens if you get hacked and you don't notice it, maybe you don't even notice that you've been hacked for a week, or 10 days or even a month. Sometimes hacking is not super obvious. If you're just looking at your site, you might only see it if you Google something and land on your site. That's a really kind of hidden sort of hack, or somebody might be using your website to send unwanted emails, they can be using your website as a spam generator. And you might not notice that just by looking at your site.

So what happens if your site was hacked a month ago, and all of your backups are from the last seven days, you won't be able to restore a good copy from that backup, and you're going to end up having to manually clean your site or pay someone else big money to do that for you. So what I recommend is having your backups for say the last week, and then keeping one from last month and one from two months ago and one from three months ago, just in case something happens to those files, they become corrupted, they're hacked, they're compromised in some way and you have to go back further to find a good clean copy.

Now I automate this on my Mac, I use a program called Hazel, which keeps all of my backups in order, she automatically goes in and deletes things and rearranges things. So I always have, you know that weekly backup, I have a daily backup for every day for the past week or for the past month and then I have older backups as well. If you're on a PC, you might check out a program called File Juggler which seems to do a similar thing. I have not used it and can't vouch for it but you will find it at FileJuggler.com If you want to check it out.

You could also just set up a reminder in your calendar to go in once each week and delete old files or set your backup program to do the same. If you are using a system like Backup Buddy, you can set that up to do something similar as well. But just having good backups is not enough. This is where we got into a little bit of time.

But if we're honest, you have to also be testing your backups. Are your backups complete, do you know how to restore your site with a backup, what's the process. are your backups current, that was what happened to us. We had backups, our server, our host had backups on our server, but they were old, they were so

outdated that they were useless to us. So make sure that you know that those backups are current, and that they are good that they're complete, that they're not corrupted, that you have access to them, and that you know how to use them if you need them.

And remember, too, that backups aren't just for your website, you also have to backup other things on your server. So that might mean backing up your shopping cart database. This was a big mistake that we made, we run our own shopping cart, we're not using something like SamCart, or Keep or any of those external carts, we run our own software. And that means that we are responsible for backing up that database. And we had not done a good job of doing that. So our shopping cart database was 30 days old. And we had to end up rebuilding that by hand by following through with our PayPal transactions and our credit card transactions and actually manually entering all of that into our shopping cart to bring our systems back up to date. So if we had had better, more recent backups, it would not have been such a big job. So make sure that you're backing up other things on your site as well.

So that can include, like I said, your shopping cart database. It might include your product files, it might include your email list. This was another mistake that we made, I couldn't contact my customers, I couldn't contact my affiliates, because all of that information was in my shopping cart, which I couldn't access. So make sure that you're backing up your email list as well. And finally, don't rely on your platform or your hosting company to have backups when you need them. Ideally, they will. But this is your business, and you are ultimately responsible for it.

I said at the beginning of this episode, that the time that we lost to this server crash was my fault. And I genuinely mean that I am responsible for my business assets. It is nice to be able to turn to my host and say hey, I screwed something up or my server crashed, can you restore it from a backup. It is great when they can do that. But it is ultimately your responsibility to make sure that you have access to those backups that you are making good backups and that you know how to use them if you need them. Because stuff happens, right? Servers go down. hosting companies may not always have good backups, and you are ultimately responsible for that.

The next thing I want you to do is to make good security a nonnegotiable policy in your business. I have seen so many small business owners, I've worked with many of them who do not have simple security practices in place. And I'm talking about

things like using strong passwords. I worked with a customer or a client at one time who used the same password everywhere, it drove me crazy. It is a recipe for disaster. Always use strong passwords in your business. Preferably use them with a password manager such as LastPass or OnePassword, then you don't even have to remember what they are you don't have to write them down. They're all securely stored in your password vault.

Another thing you should be wary of is logging into your website or your bank or Pay Pal or any other critical sites from a public Wi Fi location. Don't do that unless, well just don't do it. Don't log into those critical sites from a public Wi Fi location.

Make sure that you're keeping your software up to date. I'm talking about software that's installed on your server, but also on your computer. So this is going to be things like your WordPress installation, any plugins you're using any themes you're using your shopping cart, if you have one installed on your server like we do, all of those things need to be kept up to date, they need to be updated. The reason that WordPress pushes out so many updates is that they are plugging security holes that hackers have found. So they need to push out an update to patch that software so that it does not become infected or become a target to a hacker. So make sure that you are keeping your software up to date.

Be cautious with your email. I could do a whole show about this but you have to be careful out there. Know what the suspicious email looks like. So here's an example. Let's say you receive an email from someone and it says it's from PayPal. How can you know? Well, one dead giveaway is PayPal will always address you by your full name. It is never dear PayPal user ID, it is always your first and your last name. Pay Pal will also never ask you for your financial information, your password or answers to any security questions. And when in doubt, regardless of who the email is from, don't click on any links, open a browser and type in paypal.com into the address bar or your bank's website into the address bar and log into your account from there. Legitimate notifications from PayPal will be listed in the message center in your account. The same is true for your bank. There are other ways to get that information, rather than clicking on the link in that email.

And that's just one example. But there are dozens of other ways that people will try to break into your systems. The bottom line is this. If you receive an email from someone you don't know or that looks suspicious, don't click on it. And don't open any attachments. Reach out to them separately and ask them if that is a legitimate

email from them. And if not, how can you report it to them as being a suspicious email.

Also, remember to keep your computer up to date and to run good anti-virus software. Stay out of bad neighborhoods to such as places where you can download movies or paid apps for free. Those are oftentimes vectors for infections that can affect your computer that can then spread to other computers on your network, can spread to your software on your server, it can cause all kinds of problems. So just stay out of those bad neighborhoods, and you'll be a whole lot safer.

And finally, secure your Wi Fi network. If you have not already done that I'm talking about your network at home to make sure that other people outside your house cannot get into it and potentially infect your computers. Now let's go back to our website.

So we've talked about backing it up, we've talked about making good security, a nonnegotiable policy, but there's something else you can do to protect your business from disaster. And that is to buy the best hosting you can afford. I know that when we just get started or out there, and we're looking for the best cheap hosting, right? If you Google best cheap hosting, this is clearly something that people are looking for, because there are just all kinds of recommendations. But here's what I want you to know, cheap hosts are cheap, because they are overloaded. You will find as many as 1,000 or more websites on a single server and I'm going to put a link in the show notes to where you can go and you can enter your domain name. And it will tell you all of the domains that are hosted on your same server if you're using one of these low-cost hosting solutions.

So why is that bad? Why do we care? What difference does it make if there's 1,000 websites hosted on your server, or 10? Here's the problem. When there are that many websites hosted on a single server, you are more vulnerable to hacking, you're sharing a single server resource with 1,000 other websites. And they may or may not be doing their due diligence to keep their software up to date to keep the bad players out to keep their plugins updated to make sure that their sites are not vulnerable. And that can spread those kinds of infections can spread across a server. So if you are on a shared host, if you are on a low cost host with hundreds or 1000s of other websites, your site is more vulnerable to hacking.

Your site is also more likely to be really slow. And that in and of itself is not terrible. But it is something that Google and other search engines do not like not to mention your customers. If your customers are waiting for your site to load, they're going to hit the back button and go someplace else. So on a shared server like that your site is more likely to be so slow that customers lose patience. Google loses patience with you. And that's never a good thing. Shared hosting accounts like this often have terrible customer service as well.

So who's going to help you if you do have a catastrophic failure like we did. We got incredible support from our hosting company when our server crashed and I can tell you with certainty, that that would not have been the case if we had been hosting on a low-cost host like that.

The other problem is a lack of backups. Most of these low-cost hosts do not backup your site at all. And the software that runs your site, and I'm not talking about WordPress, or your plugins or things like that, I'm talking about the software that runs the server. So we're talking about PHP and cPanel. And those things that actually run the server, those are much more likely to be out of date and vulnerable to hackers, when you are running on a low-cost host. They just don't have the resources to keep things up-to-date, they're not going to be using the most recent version of anything, because they are collecting payments from people who are paying $3 or $5 a month. And it's just not enough to keep the system going or to keep it running at an optimal pace.

You'll also want to know the difference between shared hosting VPS hosting and a dedicated server. What we've been talking about is shared hosting, this is where you are paying, like I said $3 or $5 a month for hosting. And you are sharing a server with hundreds or 1000s of other websites that's called shared hosting, it is the lowest cost hosting you can buy, typically around $5 a month. And this is what you will find at sites like Bluehost, Hostgator, and DreamHost. They all deal almost exclusively in shared hosting, that's their business model.

At the extreme other end of the spectrum is what we call private hosting. This is where you have an entire server all to yourself. So if you can picture a server room with hundreds of computers in it, you would have one of those entire computers all to yourself, all of that space, all of that bandwidth is all yours. That's private hosting, this is probably too much for most of us, you're looking at probably $150 a month

and up in hosting fees, sometimes much, much more than that. And honestly, most of us are not running the type of business that requires private hosting.

A really good medium, though, is what's called a VPS or a virtual private server. So this is when a private server is virtually divided into smaller sections, making for better security and more control. It's kind of that happy medium between shared hosting and a private server. And this is where I recommend you land. If you are shopping for servers, look at VPS. You can get a VPS server for anywhere from $25 per month and on up. Depending on how many years in advance you purchase, or how many months in advance you purchase. If you're going on a month to month, you're probably looking at 50 bucks a month, maybe if you are buying for a year or more, you can get it down around that $25 rate.

And while we're talking about which servers to buy, which types of servers to buy, let's talk about having enough space on your server, this can get super confusing, crazy confusing, sometimes with all of the different numbers to know and bandwidth and gigabytes of memory. And I don't know what all of that means. But I do know that the one thing that you have to make sure you have is enough storage space on your server. This was why our sites weren't adequately backed up when the server crashed is because we didn't have enough space on the server to do that. And I've heard from people in the past who are having trouble backing up their sites, and nine times out of 10 it's because they don't have enough free space.

So if you think about it, it makes sense because when you backup your site, you first have to make an entire copy of it. So that means you are doubling the amount of space your site takes up. So if your site is using three gigabytes of space, and you want to back it up, you are creating an entire copy, you're doubling that you are now consuming six gigabytes of space. And if your server does not have that additional free space available to it, it can't make a good backup. So you want to make sure that you have enough space on your server to actually be backing up your site as often as you need to.

One more thing to keep in mind and to put into place regarding your hosting account is make sure that you are keeping your hosting account cleaned up. I have been guilty of this in the past. I want to test something I want to install a new site I want to play with a new theme. All kinds of things I want to do so it's super easy to just go in and create a new website to install WordPress on a new domain on my host, and play around with it. And then quite often, that project gets abandoned.

And I never go back and remove that site from my server. And that is a door that hackers can sneak into its software. WordPress is software. So it's software that I'm no longer paying attention to, that maybe hasn't been updated in a long time. And it is really vulnerable to attack. So not only is it taking up extra space on my server that I might need to do things like backing up my website, but it's also vulnerable to a hacker. So if you are like me, and you'd like to install new websites and play around with them, make sure that you go back and clean them up. Again, when you are no longer using them, don't just leave them sitting on your server, because it is not safe.

Something else that I think is really important, and I've talked about this before many, many times, but you must understand how your business operations work. You should never be at the mercy of a contractor or a team member or your hosting support, who may be offline during your working hours. It is up to you to know for example, where you host your website and how to log into your hosting account, you need to know where you buy your domains and where to log into that you need to know what software runs your site and how to contact support if necessary.

I see so many small business owners who do not have this information. In fact, I just worked with a guy not too long ago, we needed to update his DNS settings and he could not tell me where his domain was registered at. And that's just not a safe way to run business. Like I said before, you are responsible for your business, for your business assets and for keeping things safe. And part of that is knowing where to log into your hosting account where to log in for your domain, what software runs your site and how to contact support, if necessary. Don't put yourself at the mercy of a contractor like I said, because that is just not a good position to be in.

Now, I am not saying that you need to be able to log into your hosting account back end and poke around in cPanel and write code and do all of those things. That is not what I'm saying at all. That's very overwhelming. It's even overwhelming for me. But I do know enough to be able to contact my hosting support and speak to them intelligently about what's happening on my website. That's the level of responsibility that you have and that I want to encourage you to achieve as well.

The next thing to keep an eye on is to make sure that you're using tools and platforms that you can trust. Don't trust your livelihood to untested, unproven software and platforms. I know it can be really tempting to play with new software

or new apps or to try to save some money by jumping into a beta program. But be careful with that. Sometimes it pays off. And sometimes it doesn't. So you want to limit this to kind of a sandbox site. If you want to play with those unproven systems, if you want to buy a new shopping cart, or you want to test a new invoicing platform, or you want to pick up something just to kind of play around with limited to a sandbox site until it's proven. I'm going to talk more about that in just a minute. And never trust your mission critical aspects of your business to a platform that you have not properly tested. I'm going to give you a couple of examples.

So I once saw a video hosting offered on AppSumo. For some crazy low lifetime price. It looked really good. And it was really enticing as a kind of budget conscious business owner, it can be really, like I said enticing to go after those lifetime deals. But I didn't. I kept Vimeo because I'm not willing to trust this critical piece of my business to something that is unknown. The last thing I want to do is upload 50 courses, each with seven video lessons or eight video lessons. I don't want to upload all of those videos to an unknown platform and have that platform up and disappear on me. That's not good customer service for you. It's super stressful for me. And honestly, it was just easier and less frustrating to keep the platform that I've used for years and that I trust.

Another example though, we have a chat widget on the website at CindyBidar.com that does all kinds of neat stuff in addition to letting visitors open a support ticket if they need to. That is a platform that we bought at a low price on AppSumo. The reason we did that is because it's not mission critical. If it quits working, it's not the end of the world. So I'm willing to risk it in that situation. Now only you know what's critical to you, I can't answer that for you. That's something that you have to decide. But generally speaking, anything that impacts your income, I would not play around with use good, proven tools and platforms that you can trust. Don't trust your livelihood to something that is untested or unproven.

So we've talked about some of the ways that you can help prevent disaster from striking in your business. Now, I want to talk about some of the things that we changed after the server crash that impacted us. So massively last summer, we changed a bunch of things. And I think that this is going to help you kind of see how we updated our policies and our procedures to prevent such a thing from happening again.

So some of the things that we did was number one, we bought a bigger server package. Part of the problem that we had when our server crashed is that we didn't have enough space on the server to adequately backup the site. So that's why we didn't have current backups. So we bought a bigger server package, that was the first thing we did. We now keep our server meticulously clean. Like I said, I don't have any extra websites hanging around, I don't have any additional files that I don't absolutely need. On that website, we go through it. And we remove things that are not current and that we are not using. And we do that all the time.

We also added a sandbox site on a different hosting account. Now, this is not going to be something that everybody is going to want or need to do, but it works really well for us. And what we did is we bought a cheap, shared hosting account on another hosting platform. So our main site is hosted at Liquid Web. But we also run a complete copy of our entire website, the membership site, the main site, the shopping cart, everything, we have created an entire copy of it, and we run it on a different hosting account. And it's behind a maintenance wall so nobody can access it. But the reason we do that is so that we can test out new plugins and updates before rolling them out into the main site.

So that prevents that main site from potentially being damaged by an update that goes wrong or something like that. Or if we are re designing something, then we do that on the sandbox sight first, so that you're not seeing all of our dust and masks as we're, as we're redesigning something. The other advantage of that is, in case disaster happens in case our main server goes down and is down for days, all I would have to do to switch over to that other server is simply update my DNS records. And we will be back up and running in just an hour or so instead of days while we clean up a crash server again. So that was kind of the big thing that we did is we added that sandbox site on another server. And again, that may not be something that you are willing or able to do. But it is something that really gave me a lot more peace of mind.

We are also doing more frequent backups and more redundant copies. I said earlier that we didn't have a current copy of our websites. So we are more diligent about keeping current copies and additional backups. And we've also added some additional backup routines. For example, the external hard drive that I talked about earlier, that was a new addition, after the server crash. I also do a daily manual backup of our shopping cart database. That was not something that we were doing. And frankly, I'm shocked that it never occurred to me, we were backing up

that database once a month. And when you are running a multi six figure business, once a month is not enough to be backing up your shopping cart database. There are dozens of transactions that go through there every single day.

And part of the reason that we were down for so long was because we had to manually rebuild that database, we had to manually enter every single transaction for an entire month to bring it back up to speed. And that just took a long time. It was a lot of manual entry, a lot of spreadsheets, a lot of wrangling data. I don't wish that on anybody. So what we do now is we make daily backups of that shopping cart database, and we have multiple copies of it so that in case our shopping cart goes down or in case our server crashes again, the most we'll ever have to rebuild manually is one day's worth of information, which is a lot easier to deal with than an entire month.

I also started doing a weekly manual backup of my email list. So this is my email list and Active Campaign. That's not something I was doing before. It's not something that was really affected by the server crash. But it is something that I was that I became more aware of after this happened, you know, what would happen if Active Campaign shut down or if Active Campaign decided they didn't love me anymore? And they threw me out of their platform? What would I do, I didn't have my email list. And that's just not acceptable to me. So I am now, I have a task in my task manager to remind me every Sunday to go back up my Active Campaign account, and I do that it takes two minutes. And that again, just gives me more peace of mind.

So here's what I want you to take away from this episode. Because this is really important you guys, I want you to treat your business assets, your website, your email, list, your shopping cart, your products, treat them as if your livelihood depended on it, because it does. Buy the best you can afford when it comes to hosting and backup solutions. I have some recommendations for you in the disaster prevention checklists that I mentioned. And you'll find that on the show notes page.

Make it your mission to know how your business works. You don't ever want to have to rely on someone else to save your bacon if something bad happens. And make sure that you're regularly reviewing your systems. Are they still serving you? Are your backups still running? Is your server still the right size? Is there anything you need to remove or cleanup on that server, don't get complacent about that kind of

stuff. Check up on it from time to time, do your due diligence and make sure that your business is running as smoothly as possible. Because it will matter if disaster ever strikes. And honestly, it's not a matter of if it's a matter of when. So the more prepared you are, the better position you will be in when it happens.

So I would like to invite you to head on over to TinyCourseEmpire.com/43 to find the show notes, all the resources we mentioned in this episode. And while you're there, be sure to grab my disaster prevention checklist so you can add it to your operations manual. Then create a recurring task to review it at least once per quarter, just to make sure that you've done everything you can to protect yourself and your business. And finally, if you're enjoying the show, would you do me a favor and leave a rating and review over at Apple Podcasts or wherever you're listening? That helps others find us. And of course, if you have a friend or a colleague who needs to hear this episode today, go ahead and send them the direct link. That's TinyCourseEmpire.com/43. Have a terrific day everyone and I will talk to you all again next week.