Gabrielle Fontaine: Cybersecurity

Kirstin: Okay everyone, we are ready to get started again with Gabrielle Fontaine. I am really excited to introduce Gabrielle. She is the founder and manager of Bookkeeping Direct, a bookkeeping firm which has been running 100% virtually since 2003. She knows a whole lot about a whole lot. And she is considered one of the experts in the virtual bookkeeping industry. We are so glad to you have you here today, Gabrielle.

Gabrielle: Well, I'm excited to be here. So, thank you. And I love how it's like since 2003.

Kirstin: I know. Well, I mean-

Gabrielle: If I want to really scare you, I started my business in 1990. Yeah, that old.

Kirstin: Well, it was so funny, because I actually was thinking about doing bookkeeping from home back in 97, but I didn't know how to do it. And I wish I would have found you sooner.

Gabrielle: Well, I wish you did too.

Kirstin: Well, I will go ahead and turn over the presentation to you.

Gabrielle: Well, thank you. And I will turn on my screen and I'm from Sunny, Florida. So, I have to follow suit here with Mark and Ben Day. They both had exciting topics. And mine is a little bit of a different type of topic. So, let me share my screen here. And hopefully it'll work. Can you see my screen?

Kirstin: Yes.

Gabrielle: Oh, yay! Good. Excellent. Well, now we're shifting gears. And we're going into the dark side, the behind-the-scenes stuff that us as digital or virtual bookkeepers need to pay attention to. And I would say now in our work from home world, because it's funny back when I did first start doing the virtual bookkeeping back in 2003, I didn't realize I was ahead of my time, but at the time, a lot of people wanted to work through the internet, it seems great, have all that flexibility, it's wonderful. But then as we know, within the past year, whole lots of people are working virtually that even weren't planning for it, including many of our clients and even ourselves, maybe some of us were semi virtual, and then we've had to really go full on for the pandemic. So now as virtual or digital bookkeepers, 21st century bookkeepers, we need to be paying attention more than ever. So that's what we're going to talk about today. As usual, if you've ever been on any of the classes that I've done, I have a ton of information.

Gabrielle: But you know what I'm going to do, in fact, Kirsten is going to help us with this. Is, I have a couple handouts. So, I don't want you to worry about taking notes, because I go through a lot of information. So, she's going to share these with you. And even if for whatever reason you have trouble downloading them, don't worry, you will get them you're going to get a copy of the slides as well. So, I want you to sit back and just think about your own practice as we go through all this information and just zero in on the pieces that are going to be the most relevant and most important for you to be thinking about right now. That's why we're calling it the essentials. So, our objective today is really to see the risks that we're up against. And they're changing, because we know the world is changing. It's funny before the pandemic happened, we were already our profession is shifting because of technology.

Gabrielle: And in some ways, that's been a blessing because we can do so much more online now, but because of the pandemic in the cybersecurity realm, there's a lot that is changing as well. It's changing all the time, but certain areas that we'll talk about, it's shifting as well that we need to pay attention to. Also, we want to discover the areas right now that we need to look at and the steps to take to lower the risk of a breach. And also, my goal is for you to walk away from this session, especially before lunch because I don't know about you, if you're on the East Coast, your stomach starts rumbling around now. But we're going to hopefully keep you engaged so that you can take some action, have some ideas on what you want to be doing to use what you're learning, because today you're investing a lot of time, let's use it to really benefit ourselves and our clients right away.

Gabrielle: So, I got to give you a disclaimer first on this topic for cybersecurity. And that is that first of all, it's a huge topic and there's many, many aspects. It's actually a whole industry, the cybersecurity industry, so just to realize the whole business is surrounding cybersecurity. So, we're just going to focus on what's important to us as bookkeepers right now. And I also have to give you a quick legal disclaimer that this is not legal advice and I am not officially a cybersecurity expert, but this information is really just from what I've learned through the years, because I'm that old. Yes, I've been virtual since 2003 and I've done a lot of research and I have experience in this world. And then, you should of course, anything that you learn from here, if you think is going to make an effect on your business, you should be consulting as well any professionals in this field, so that you can make a wise decision for your business. Because obviously, this is for information purposes, but I don't know your particular business situation. So just realize that.

Gabrielle: All right, so what we're going to cover is what has changed? Why is it that it's more urgent now than ever? Also, this work from home concerns, which is that extra layer that some of us if we weren't working from home before, or even if we have for a while, and we just haven't really thought about this that we'll take

a look at. And then also the action part. What can you do now to protect yourself and your clients? And then we're attempting to leave some room for some Q&A, but this is going to be a bit interactive, because I want to ask you a few questions as we go through and see where you're at on this topic. Because again, cybersecurity is not so sexy, like pricing and client meetings. So just stay engaged, because you will get a lot out of this if you are focusing in on it. So if you don't know who I am, you did see a quick bio for me.

Gabrielle: I started my business actually in 1990, been virtual since 2003. I am in the QuickBooks world, and have been for quite a long time, online for quite a long time. And as you know that I do classes online. And when we used to have conferences both in the US and the UK, I've done speaking at conferences and most of that's been put on hold, but I expect that we'll be able to do that again. So, getting into the meat of our meet and greet here on this particular session, what has changed? Why is it so urgent now? Well, as you know, COVID-19 has actually raised cybersecurity risks for us. And that's because they're really taking advantage of the vulnerabilities that have come up because of how quickly COVID-19 to cold really on the world and including the working world. So, Accounting Today said that with the increase in the remote workforce and ongoing COVID pandemic, a 300% increase in cyber-attacks notice on accounting practices of all sizes.

Gabrielle: So, we fall under the accounting professionals that are being targeted. And that includes the small practices. So maybe you're relatively new in your digital bookkeeping business. And I hear this all the time that we think, "Oh, they won't come after me. I'm so small, I only have a handful of clients." That is not true. No bookkeeping practice is beyond the radar of these bad actors or the attackers. And in fact, in much of the research, because I've done many, many webinars and speaking live on cybersecurity, so I do a ton of research on it as well. And there was one that was kind of chilling to the bone that I saw not long ago, that it was a presentation by someone who was one of these hackers and then he kind of came over to the good side. Now he has a career working with cybersecurity firms, but he said that it's like a mantra with these attackers that if there is a vulnerability, it will be exploited without exception. That is their rule that they go by.

Gabrielle: So often they will break into things just because they can and then other times more and more, they have a profit motive. So just know that even if you have only a few clients and it's just you, you still need to be paying attention to the cybersecurity landscape and how it affects us as bookkeepers. So why are we a target? Well, the big reason is because they're following the money and we're involved with the money for our clients. We also handle sensitive business and personal information. And as we know, personally identifiable information is like currency for them on the black or they call it the dark web. And also, in general,

we're easier to crack than larger businesses who have deeper pockets to have security protection, because it can cost a lot. In fact, CNBC said that small companies... Sorry, I'm terrible at reading slides. And I know most people don't want to be reading them anyway. But the amount of small companies, the accounting industry is among the most targeted, healthcare is another one and government. But so, we're right near the top of the list.

Gabrielle: And phishing emails in particular, are what they use, it's what they send to us. And we're going to see that as we go through this. And I've experienced it myself. It wasn't recently under the pandemic, it was a few years ago, but it was one of my clients, her email was breached and she didn't mention that, she clicked on a phishing email, they got her email credential somehow, she was away traveling and I was actually traveling at the time too. And I got an email asking about her balance. And I thought it was strange because she's on QuickBooks online and she can see her balances and she has online banking too. And I just thought it was strange. I questioned it because it was strange and come to find out it was the hacker impersonating her and wanted to do a wire, which of course I couldn't do. But we were able to help secure the client immediately because I contacted her virtual assistant who also contacted her IT guy and we got it all taken care of. So, there was no loss involved.

Gabrielle: But it was a little shaky, because it was being sent, he had my name, he knew I was her bookkeeper. So just know that it can happen and it's usually through email. So, the point here, and we will talk more about this is our client's risks are our risks too, because that's how they'll come after us very often, they'll also try to get us directly too. And this quote here, which is quite new, it was a webinar that I watched just last month on the SBA, the Small Business Administration from a cybersecurity firm that said small businesses are the most vulnerable cybercrime targets. Unlike large enterprises, small businesses may not have adequate resources to protect themselves. And that's becoming more and more that we become more attractive to the bad actors. So, it usually starts with our clients. And a question to you now is to stop and think, do your clients have adequate protection in place to protect against the most common cyber-attacks? We as digital bookkeepers have to be thinking about, we have to protect ourselves and make sure we're protected.

Gabrielle: What about our clients? Because if most of the breaches come in through to us from the clients, how protected are our clients? What role are we taking in helping to protect our clients? And now taking a look at COVID, did our clients have to suddenly go virtual? Are they trying to juggle the equipment and the software to work virtually and try to adapt quickly? That's where much of the exposure is. So, the stakes are higher now. And they have new opportunities to attack us, as we said, because it's the shift that we have to do. And most small companies with this shift aren't thinking about the security issues for the most

part. And many of the home devices, in fact, I read an article that was saying that many employees of larger companies that had to go home and now they're trying to, they can't really provide the equipment for their employees, so they're using whatever's at home. And they said, in some cases, the equipment is a decade old, they have old operating systems.

Gabrielle: So, we'll talk a little more about that. But these bad actors are exploiting all of these vulnerabilities as opportunities for them. And in the first half of 2020, nine million email threats related to COVID-19 were sent out and 92% of those were spam. So again, that's actually a great example of how much of the breaches happen. The number one way is through email, spam email. And then also with the PPP and economic stimulus going on here in the US that they're using that to trick us and maybe you've seen it, I've definitely seen an increase that you'll get these what they call them smish. Instead of phishing emails, you'll get smishes, which are SMS phishing. So, you'll get these text messages that will say that your bank and you've been locked out, you need to click here and log in right now. Any of those, that's all bad. Are your clients falling for any of those? And then also voicemails will come in that are expounding on this talking about something related to either the stimulus or on vaccines.

Gabrielle: So, we have to pay attention or our client's going to fall for this, because that's a risk to us. And what about now those working from home concerns? Well, this is a report, which you will get in the handout, there's a link to this report that it's from Malwarebytes, which is a cybersecurity company, been around for a long time that they help remove malware is what it's called, the malicious software. And so, they surveyed from COVID-19, many of the companies they're working with and noticed these top three concerns and challenges that they have, which is some of which we mentioned, of them trying to get their employees set up to be working from home, also to deal with all the personal devices that they're using. And then just figuring out how to keep the business running with the remote communications. So, the clients are all trying to juggle all of these things at the same time.

Gabrielle: So, these are concerns that they have now all of a sudden with their employees, but think about us if we're working digitally and we've had this in the past, where they will be afraid of working through the internet, or afraid of security issues, we have to now be concerned, are our clients going to be worrying about this now? Or how can we give them the confidence to realize that we can provide them security? Because we got this. We've figured it out, we've thought it through and we found solutions. So, it's a double whammy here and that we have to be thinking about our working virtually if we're hiring virtual bookkeepers. We need to be thinking about this as well, but also think of it through the eyes of your client, you can use this. It's kind of a side point, but you

can use this almost as a sales angle too, on how you are superior to other bookkeepers who may be unprepared for working through the internet.

Gabrielle: So, the personal devices, this is a true risk, is that if sudden shift happens, now they have to start using the family desktop computer, or you know their son's laptop to start working. They're sharing devices, they may not realize that that could cause... Because if you're using cloud-based software that maybe there aren't protections and information now may be going on these local devices that others will have access to. Also, inadequate security on the tools that are being used those cloud-based tools. And an example of that which most of us heard is early on, when everybody went to the video conferencing and started using Zoom, there was security issues where there was Zoom bombing. People were getting into meetings that shouldn't have. And so, Zoom as a company had to scramble to up their security. So, as we said, remember those bad actors, they look for vulnerabilities, because their goal is to exploit all of them. Also, a lack of adequate cybersecurity protection on the home networks.

Gabrielle: If we're using old equipment and the old software, it might not be up to snuff now for the protection of all the information that's passing through. So, we need to make sure that's up to date. And then also off boarding of remote workers. And you may think of this, if you have a virtual team, that if you end up having someone leave you, are you paying attention to what access did they have? Are you turning all that off? Are you changing the passwords? These are the things that are top concerns for companies from the pandemic having to shift that maybe it's stuff that we need to be thinking about now, even if we were already working virtually, are we looking at all of this? Because it's the kind of thing that we might not be paying attention to and that's what the bad actors are counting on. So, what has actually happened from that report, it showed all the concerns that the companies were having, but this is what's happened within the past year with these companies shifting to go remote.

Gabrielle: In that, there have been 23.8% cybersecurity breaches and malware attacks. And there've been 19.8% that faced a security breach as a result of a remote worker. So, we need to be sensitive to this for ourselves and for our clients. And of course, like I said, and then we can work that into onboarding new clients to help them realize that we can provide that security but we've got to do that first. We have to think about it ourselves, because these are actually very big numbers, if you think about it. So, what can you do? I hinted a little very teeny bit about what you can do so far. But let's go through some key areas that you might be facing right now. So, the biggest risk of all, we said email's big and you're going to hear that, but the absolute statistically biggest risk is human error. And it becomes because we're not paying attention. We're trying to get the job done. We're trying to make sure the numbers balance, we're trying to answer our

client’s questions, we're trying to bring in new clients. We're not thinking necessarily about how we're doing.

Gabrielle: And we're going to talk a little bit more about a particular vulnerability that we as bookkeepers and if we're doing taxes as well, that we have. But 95% of cybersecurity breaches are due to human error. And so, we need to realize that. So, the biggest defenses pay attention, or I always think of that joke that they always have be alert, the world needs more alerts. That's absolutely true. We all need to pay attention. And especially as bookkeepers, we're in the trenches where the money is moving around, it's very important for us to be that trusted person who is paying attention and has our clients back as well as our own. So key areas of focus are email and attachments, top of the list. Also, login credentials, those are really the two main ones. If you're already feeling like, "Oh, my goodness, there is so much I need to think about here," focus on these top two, that's going to get you the farthest down the trail of protection.

Gabrielle: And then also, as we've hinted that outdated software, equipment and devices, you really can't keep things too old because that will increase the vulnerabilities. When the companies stop supporting... This is a little tidbit. When you have operating systems or browsers, or anything like that, when the software company stops supporting that software, it's time to upgrade, okay? Because if you don't, what happens if there are new vulnerabilities that were unknown before, because the software is no longer being supported, any updates or patches to fix it will not be available. So, you'll be sitting dark for any hackers that know about it. So just so you say, stay just ahead of being obsolete, if you must. Also, backup and recovery plans. Do you have one in place? What happens if you had a breach tomorrow? Do you have a plan on how to respond to that? And I will say as just a caveat I guess here, is that nobody likely has everything handled, we're just trying to do the best we can do.

Gabrielle: So, focus in, first things first, focus first on email attachments and login, how they're being handled. And then you can graduate to the other parts. But I will also give you some good hints going through on how to handle some of this easily. So, handling emails and attachments. Email, as we said, is a major problem and it's because it's so convenient. It has been... We're always hear like, "Oh, email's going away." It's still around, it's still preferred by so many people. And yes, we have some tools that can help us reduce that. And that's a good thing. But realize that email is still going to be a risk in general. It's not private and it's not secure. And then the thing I say is think about it, whenever you're sending an email, it's like sending a postcard in the mail in the physical mail, where you're writing a note, you wouldn't write something secret on that, because you know that as it travels through the mail system, other people could see it, nosy people could read it.

Gabrielle: So, think of it that way. When you send email, you and the recipient may not be the only two people who see it. There are others, it goes through a very convoluted path if you ever dig deep into how email works. So just realize it's not private, even if it feels like it is. So never ever email sensitive information, except if you are using encryption on your email, so that it's encrypting both the message and the attachment and that means that it's keeping it encrypted all along and when it arrives. So, there are easy ways to do that. In the handout you'll see one of them that I use that's very simple to use, is called Virtru V-I-R-T-R-U, I believe is how it's spelled. It's very convenient, useful and helpful. There're many other choices too. But if you have to send sensitive email, that's an easy choice to use. Also provide training to your team and clients. And I also recommend using a secure portal for file sharing.

Gabrielle: Because email's easy and simple, and our clients I have clients too that still after years, they'll decide that they're going to email me something. And I slap their hand, but then they'll be like, "Oh, yeah, I forgot." And they'll email sensitive tax information. And so just realize we have to continually train our clients, in my case for them to use the secure portal instead. But something else to pay attention to that I've seen during this time of year, we just came off of 1099 season, we are going into tax season and this is where now everything flies, we have a strange year as well for tax season. This is when we also will get requests from third parties, such as when we were trying to get the W-9s that could hold Social Security numbers on them. Do not email that information, do not ask for it by email, we've seen that all the time. I also had just recently, one of my clients is doing some financing work and the mortgage company. The mortgage company wanted her bank information and they wanted it emailed, for the ACH information.

Gabrielle: And it's like, "No, they sent the form." And it was like, "No." So, you have to provide an alternative that is secure for even these third parties. Just because... And I've fought with some software companies who should know better asking for sensitive information to be emailed. And they tell me, "Oh, that's just the way we always do it." Their back office isn't paying attention. And you have to push back and say, "No, I do not share that information by email. It's not secure. Let's do it this way." So just putting the heads up, you can push back even on so called authorities on how sensitive information should be shared. So just keep it in mind because it happens all the time. And I get floored by how often this happens. So also, for recognizing phishing emails, because as we saw, the vast majority of the breeches that come in is through email and they usually want you to click on a link or open an attachment, or both. And we've seen lots of this lately again, because a COVID.

Gabrielle: But something that you have to... If you're not sure, because the phishing email's starting to look really, really good. They're really good. And the thing that makes

it worse too, and Intuit has done this, that they send out an email to us that is genuine and it looks like it's a phishing email. So, the phishing email and the genuine emails are starting to cross over so that that gets harder and harder to recognize. But one way to look to recognize it, is when a message comes through and has an urgency to it and they need you to click this right now. That is an earmark of a phishing email, because they don't want you to think about it. They don't want you to be paying attention. So, it can appear that it's coming from a company that you know, or websites that you work with all the time.

Gabrielle: And again, often the way this can happen is if the bad actors not to freak you out. By the way, just so you know, when I do these webinars afterwards, I start getting paranoid. Because I think that the bad actors know that I'm teaching to protect you, so now they're going to come after me. But is that they will often if they get into a system, whether they're in your client's system, somehow the client doesn't know it, or they get into your system and you don't know it, they don't automatically let you know and lock things down, unless it's ransomware, but they will sit and watch. They'll get this backdoor and they'll watch. What are the emails that are happening? Who are you interacting with? And what websites are you going to, so that then they will create a spoofed site or they will create a spoofed email, so that they can grab your information. So not to freak you out, because it does get a little scary, but to know that a phishing email can look really good.

Gabrielle: And they will imitate the IRS, particular banks, any apps that you're using, there's a lot that you would see for DocuSign, Dropbox, Google, Microsoft, they imitate all of them. And so, my rule of thumb and sometimes it's been genuine email. But my rule of thumb is, if it doesn't look right, something about it, it just doesn't seem right, you can check the address on the email, where did it come from? And check the spelling too, because sometimes it might be like if it was Intuit. Intuit and then have an extra eye on the end .com. And you got to pay attention. Is it exactly the true URL on that email address? And if in doubt, the easiest way is, if it's an online app that you're using already, anyway, just go login independently.

Gabrielle: They're saying, "Hey, your account's been locked, you're going to log in now and do whatever." Okay, maybe it really is, go login independently, don't use the email link. And then that way, if there's a problem, it'll show up when you log in. So, that's the easy way to protect yourself. And then look for strange expressions, bad grammar, spelling errors, or formatting that seems off. And I have an example to share with you that it was one that I got. And it was, again, pre pandemic, because it's hard to get all the stats during pandemic, so it was last year, or 2019. But it came from Stripe and I have a Stripe account. And I would get messages from stripe all the time. And it says your stripe payout

failed. You're like, "What!" And I had had situations where Stripe for whatever reason, would hold the payments for a while.

Gabrielle: So, this kind of caught my eye, I was like, "What!" For split second because they had the branding here. I thought, "Oh, is this real?" And here's what Stripe does. Often stripe doesn't use your name. So, they're imitating it might not be so you notice there's urgency here. The payment failed, I got to update my account, looks okay at first. But then when you stop and look at it for a minute, notice down here it says San Fran. Who puts San Fran? An official company puts San Fran on there? And see they have my email address, but then here's something else. They're using Constant Contact to send the email. I'm like, "There's nothing here." And then this of course, all look strange. Look at the email here, the address it's coming from. That's not coming from Stripe. So, I knew that it was fine. But it takes a minute. If we're busy, we're running through things, we could not be paying attention. So, we have to be paying attention to what we are doing so that we don't get caught. So how about handling of login credentials.

Gabrielle: I'm going to watch the time here because I want to handle any questions that come through. But logins are valuable. It's like money to the hackers. That's what they want. So, we use logins all the time, so we have to be protecting them. We use them for our business software, clients' accounts, client apps. And even if we have a team, there may be different logins that we're all sharing, hopefully not, but sometimes you have to. Review how your logins are being handled and how are they being stored. You want to pay attention to that? Because there is exposure. I talk to a lot of people because I teach this and know this and I hear like well, what are you doing with your logins for the different apps that you're using? And they're like, "Oh, I have it on a sticky note on my computer, or I have it in a spreadsheet on my hard drive."

Gabrielle: And I'm like, "Oh, so is their encryption on your hard drive, or is the file encrypted?" "Oh, no. And it's a family computer, which is like, "Oh, no, don't do that." If somebody hacks in and they find that, they got the keys to the kingdom. So, I do have a list of do's and don'ts for handling your login credentials. I'll go through them quickly. But again, don't worry, just kind of listen for one or two that might be helpful to you, you will get the slides. So, we have, don't send login info by email. And I've heard people send and I've in the past before I knew better, is that they'll send, here's your user ID and then in a separate email they send here's your password. That's not recommended. What you should do is send their user ID and then send the password by a different mode, maybe by text or send it by an instant message if you're in some instant messaging or call them on the phone. Just don't do it all together.

Gabrielle: Because if for somehow someone is monitoring email on your site or theirs, you don't want them to get that information. Don't share logins if you can avoid it. I

do realize sometimes we have to, so it's super important that it's protected. Use the same password on multiple sites. Don't do that. Don't use password managers that are built into your browser. Although they're better than nothing, they're not that secure. Because if bad actors break into the browser, they'll have access to it. And definitely don't put credit card information in your browser either. Don't store logins in an unencrypted Excel or Word document, as I said, or written on a piece of paper that someone else could get ahold of. Some dos on the positive side is change your passwords regularly. So, you don't want to be trying to remember them all, you want to use a different method here, use long passwords with letters, numbers, and special characters that are even sentences on a few key passwords that you may need to remember, this is what is recommended, keep it as a long sentence that is using these different characters in it.

Gabrielle: And don't bend your brain trying to remember all of your passwords, because I think it's impossible. Use a dedicated password manager in your handout, and most of us, I hope are already using it but use like LastPass or RoboForm, they will generate good passwords for you too. So, you don't have to always come up, you only need to know your master password that you should memorize. Do not use a dedicated pass... Or do use a dedicated password manager. And then also use secure sharing, if you must share. And you can do that both with those password managers, so that then basically, if you have someone on your team, you need to share a password with them in LastPass, you can share it so that then they can use the credential, but they don't see the credentials. If a hacker really wants to break through on that they can, but again, it's an extra layer of protection, as opposed to just giving them the logins. Also, you can turn it off so that if you stop working with someone, you cannot share it anymore with them. And I would recommend changing the password as well.

Gabrielle: Also, do turn on multi factor authentication. It's also called two-factor authentication, it can be a pain in the neck, that is when every time you log in then it wants to send you either an SMS with the code, or you're using an authenticator app where you're getting a code and you're putting it in, do cannot that, it's a pain in the butt. But it adds a ton of protection. And again, that hacker guy that I heard from, he said that that's a game changer. If we turn on the multi factor authentication, they can't get through. So do use that, especially on your most vital logins that you use. So outdated software and devices, operating systems, you want to keep those up to date, including on your smartphone and tablets, you want to turn on the automatic updates, that's the easiest way to do it. Also, with older hardware can have vulnerabilities such as your routers, modems, and firewalls. So, you want to keep those, as I say ahead of being obsolete.

Gabrielle: And if sensitive information is on your hard drive, you do want to be using an encryption app for that or use Windows 10 Professional, does have it, it's BitLocker, I think is what it's called. You can turn it on, but by default, it's turned off, that will encrypt your hard drive so that the bad actors can't access it. Then the backup and recovery plan, you want to know what do you do in case something happens to your information backup, backup, backup, you want redundant, that means more than one of the same. So, if you have information on your hard drive, you want it to be on an external drive and on the cloud. And I'd recommend using an automated program for that, giving you a lot of the tools that are in the resources. But Backblaze is a good one, Carbonite is another one that can be used for the automatic backup of it. So, if you're using cloud-based tools, and they may be always updating and so forth, that's helpful. But if you have anything on your local drive, you definitely want to be using cloud-based backup system.

Gabrielle: Also, have a plan for what happens if you do get a breach? Do you know? Sit down and think about it. I would love to go into that, but we're going to run out of time. You can look up that online and find it. But the best first step you can take and all of us should do this again, my recommendation is even if you're a solo practitioner, get cyber security insurance. Before some of us kind of did it, we get ENO, but we weren't sure if we were going to have cyber, now with the pandemic, get cyber insurance because they can help you if something happens, they can help guide you. And we'll hear more about that later today when you get the session with Ben and Jock. So, let's move on. So now, I have a few true case studies of things that have happened to people in our field, bookkeeping and taxes. And watch what happened and think about how could you prevent it if you were in their shoes. So, the first one, and if you saw my cybersecurity class, you probably heard about this.

Gabrielle: Her name is Jessica Pillow, who has Pillow May Accountancy, and she was the victim of a successful phishing attack. It's her and she just had a couple of bookkeepers with her. The client emailed a bill to be paid. Nothing unusual, right? She said, "It even sounded like our client and we processed it as normal. And it cost us thousands." And that's because the attacker had infiltrated the clients email system very much like mine, I got that too from my client that had been infiltrated. And then they skillfully impersonated the client to trick the bookkeeper. And that's what it is. They want to make it as authentic and do something that you normally do again and again. So, the hacker I had, he didn't stick around long enough to learn that I didn't do wires. But in this case, they paid the bills for the client.

Gabrielle: So, what lessons could we learn from that? And if we got a minute, I'd like to hear Kirstin, if anybody puts in what went wrong there with Jessica Pillow? What caused that... In fact, I'll go back up. What was the cause of that vulnerability?

Because it's something she got it in emails, she didn't know it was impersonated from her client. The URL was correct, the email was. So, Kirstin if anybody mentions to you in the questions box right in, why did this happen to her and what could she have done to prevent it?

Kirstin: Yes, some people are entering in, no is secure AP, approval process.

Gabrielle: Yes.

Kirstin: Yeah. She didn't pay attention to the email. The client's email was hacked. She wasn't having the client upload unpaid bills to their secure file sharing system.

Gabrielle: Yes. Very good.

Kirstin: Was that a new vendor? I would have asked if it was new, confirm with the client. Yeah, lots [crosstalk 00:42:43]. Check with the client. Yeah.

Gabrielle: Yeah, that's right. Excellent. Great job everybody. Great job with that. So, I have down that. If providing AP services, then you must have controls in place. And you guys mentioned most of them. So that's great. There are payment apps that can help with that and make it much easier and secure. Also, using email communication with clients on sensitive transactions, makes it easier for bad actors to intervene. Someone said they should be uploading those bills to the secure portal where it would go or if you're using receipt bank, or however you're getting the information, she should not have been receiving the bills by email. So, consider using non-email client communication, practice management software often has that included or even in Slack, that has at least some protections and it's better than email. So, here's another example that we have, is of a tax preparer who received an email from an attacker posing as a client. And this preparer was trained to recognize phishing emails but didn't recognize this one. The message was well crafted and sent during the height of tax season. And if you've ever prepared taxes, you know how crazy things get.

Gabrielle: So, the attacker said that they had information that they wanted to send by email, and the preparer responded and said okay, so then the attacker thereafter sent a file saying that it was this information that was needed for preparing the tax return, the file was opened, malware was released onto his computer and they stole bank information and the preparers contact list. The banks were accessed, money was lost and there were fraudulent emails that were sent in the name of the tax preparer so then it went further out killing reputation as well. So, this one is really serious, really scary and they couldn't retrieve the money either from what happened on this. And something I just read too while I was preparing some of this, is that it takes a hacker if they get bank details, it takes a hacker nine minutes to access and get the money from a

bank account. So, there you go. Lessons we can learn from this, anybody? I want to hear anybody who does taxes. Again, I should go back so you can see the details on it. And Kirstin, what are we hearing?

Kirstin: Yeah, I know what I noticed right off the bat, because I get-

Gabrielle: Yeah, because you prepare taxes.

Kirstin: I prepare taxes and so I get some of these emails. Someone said, use a secure portal right off the bat.

Gabrielle: That's right.

Kirstin: One of my question is, because a lot of times when I receive an email like this, it's from someone completely out of the blue that I've never talked to before. I know that that won't completely solve the problem, but a lot of times, that's how it goes. "Oh, hey, I heard about you from James..." And I got this just the other day. "Here's my tax information, how much do you charge?" Or something. And they were wanting me to open it up. And so I replied with, "James who? I know lots of James's; I'd like to thank them." "Oh, I don't remember their name, but they were a retailer." And I'm like, "Yeah, right." So anyway-

Gabrielle: To me, that's chilling, because now you're having a conversation with a hacker.

Kirstin: Right. Yeah. I'm like, "Yeah, nice try." So, let's see. Yeah, pretty much secure portal is that. And then an established relationship too.

Gabrielle: Yes.

Kirstin: Because sometimes people are legit clients, but they are ignorant themselves. Because then I'm like, "Hey, feel free to set up an appointment with me blah, blah, blah." Automatically. Yeah, exactly. Exactly.

Gabrielle: Yeah, very good. Very good. Well, at the busiest time of year, we need to be paying attention, because that's when we're more vulnerable for sure. And mistakes can happen. In fact, I had this with the 1099s. I had an accounting firm email me and said they needed a W-9 for one of my clients. That client has a Social Security number, it's a sole proprietorship. So, then I was like, "Seriously, you've got an accounting firm?" This was a larger accounting firm, on the 29th, asking for this. And I was like, "Yeah, I ain't giving it to you by email." I sent it to them securely. But it happens, because it's busy time, they've got a deadline bearing down. We need strict guidelines on the policies and procedures on how we're going to be handling these documents, and we can't vary from them. If they're like, "Oh, just this one time." No, go use my portal.

Gabrielle: And you have to make sure your team is up to speed on that as well, if they're feeling the deadlines, as well as your clients, there's education that really needs to be part of what we're doing for our clients. And then any dealings with third parties, as I had said like in this case, that accounting firm that came to me. That is not my client's accountant, it was because they were the accountants for one of the vendors of one of my clients. So, here's your action plan on this over a lunch break, you're probably getting a little hungry, make a list of the top one to three vulnerabilities that we kind of touched on or talked about today, set a date on your calendar when you're going to sit down with a clear head and work on it at least to get a plan down. What you're going to do next, your next step. And then use the session handouts that I'm providing you as a guide, they're both similar, you can use either or both.

Gabrielle: One is just a checklist, the other one's kind of a checklist with some guides to take some action and some resources. Just do something to move in the right direction to help protect yourself and your clients. And just realize that nobody is 100% protected, this is changing all the time. But the small simple steps of dealing with the email and dealing with the login credentials, those are huge, that will help protect us. If anything, turn on the multi factor authentication on the apps that you're using and just accept it. That's the world we live in as digital bookkeepers, we need to pay attention to this and protect ourselves, our clients and everyone we touch, because that way we become far more valuable to our clients because there are many bookkeepers and accountants who are not doing this. So, with that, I will leave it to, are there any questions Kirstin that you saw that we can talk about until everybody dies of hunger?

Kirstin: We do. We do have some. What are some examples of secure portals?

Gabrielle: Well, the one I use and have for many years if you followed me is SmartVault, is a standalone one. But there are also practice management software that will have portals built in more and more. And they can go from the low end to the high end. I know on the resources, one of the... They've been around a few years now, and it's really for very small practice and it's reasonably priced is in Encyro. And that does with email, it does encrypt, it's kind of a hybrid. It does encryption with email, but they also have it so you may have it go from your website as a secure upload place where the clients can upload and it's all encrypted and protected. So, that could be a simple portal. Pixie is one that I'm using now and they have that feature that's in there.

Gabrielle: I know Carbon, I believe. Carbon, if David's on here, he'll know. There's lots of them. The practice management software often now has secure portals built into them, but if you need a standalone, SmartVault will do that. And I think some people use ShareFile, but I know something changed with ShareFile. And it's often out of our price range. So those are few ideas.

Kirstin: Liscio is another one that I've started using.

Gabrielle: Liscio is another good one.

Kirstin: What about Google Drive or OneDrive?

Gabrielle: I always get asked about that.

Kirstin: Dropbox. Yeah.

Gabrielle: I have a mixed answer. I've always said that we shouldn't be using free consumer level tools for professional service that's handling sensitive information. However, I will say because and this is... There's always a little bit of a silver lining in the dark cloud of the pandemic, we've seen some of these companies because of the remote work that they've upped their security. I've notably seen that with Dropbox. Dropbox has improved the security that they had on the consumer level. So, there's a long way of saying that there is security on those cloud-based file sharing methods, but they're meant for pictures, and for videos and people sharing stuff with each other. They're not really meant for tax forms. So, I would say check on their security and it's not going to be like bank level security generally. But you want to dig in and see what are they offering? How secure is it?

Gabrielle: Maybe you need to just go up to a business plan, if you can afford it, but just have as much security as you can afford, is what I would say on those. I used to say don't use them at all. But they've gotten better and I know a lot of people use them.

Kirstin: Right. For password managers, a lot of times they will be like a Chrome extension. Is that different from the built-in password manager in Chrome?

Gabrielle: Yes, it is. It is. And actually, it's very convenient. In fact, I've used RoboForm for many, many years, and they've improved and it's RoboForm anywhere. And it's great because it'll sync to all the different devices. But it's got the protection, because it's only sitting in the browser, but it's not giving access to the browser of all of your information. All of your information is on RoboForm's servers, and I know that LastPass is somewhat similar in how that works.

Kirstin: Do you have verbiage to use with your subcontractors, your employees, et cetera, to provide them with expectations for security from working from their home? How do you go about having that conversation?

Gabrielle: It's a good question. And again, before people didn't worry too much about it. And it's something when you're working with a virtual team, we have to be

paying attention to. I don't have specific verbiage, but it's more like I ask them when you're interviewing with them, and I recommend putting together a little checklist based on the stuff that is in the handout, come up with your own checklist too to say, "Hey, are you using a password manager or..." It's actually easy when you're working with a team, I just kind of control it, that I use LastPass for the sharing of anything that has to be shared with the virtual assistant, I've had it that sometimes they have to log in to some of my logins. But as far as I just put a checklist and the standard you let them know. Do you have errors and omissions insurance? Do you have cybersecurity insurance? Because if they're a subcontractor, if I'm working with that. If they're an employee, you want to definitely make sure you want to know about what equipment are they using, are there others in the household using those?

Gabrielle: You just got to let them know. I don't usually give scripts on things because I speak from my heart. So just let them know, "Look this is serious, we're doing this, we need to protect you and your family, we need to protect my business and we need to protect our clients. So, these are the things that you need to have." So, I would do that with a contractor or an employee.

Kirstin: Okay. And then on the flip side, how do you handle it with clients who just are not getting it? You've had the conversation, "Hey, use my secure portal for this." And they still email you things. I literally had a client email me their credit card number, complete with the three-digit code on the back, all in the same email. Or they text to me or whatever. How do you handle that when they just are not grasping this concept?

Gabrielle: Well, is it Tony Robbins, who says repetition is the mother of something. But to get it down, you have to say again... Mother of genius or something. But you have to get it, you got to tell them again and again. I've had clients who have... They had contractors, but I teach the clients that they go take a screenshot of all their bank information and then they attach that and email it because they want to... I was like, "What are you doing?" And then I do have one client who repeatedly year after year, he will always send things by email that has his and his wife's Social Security numbers on it. And I tell him year after year do not do that. And he's like, "Oh yeah, I forgot."

Gabrielle: So, when they do it, all I do is become the broken record. I'm like, "No, you're supposed to be uploading it, I do think using something like Liscio." The best way to do that is if you can move... And I'm not saying it's easy and I haven't completely accomplished it either. Is moving the clients to communicating with you through Liscio, or another method, not email. And that would solve that.

Kirstin: Yeah, that makes sense. That makes sense. Let's see. If you have to encrypted email providers or something like that, is it safe to send email from Google to Google or... Let me see if I can find that question again.

Gabrielle: Because if you're sending it encrypted, like I said, I use Virtru, what happens... And they don't have to be on it, they can use any email for that. And again, it's trying to use separate programs. Maybe what they're asking is if Google offers to encrypt an email, but it has to go to another Google user or something. I wouldn't mess with that. Get something that what that app does, is the encryption, that is its job. So not as an add on feature. Although I say that and I know that SmartVault has a plugin to Outlook that will send emails that will be encrypted. But still, security is their thing. But basically, with the Virtru, what it does is when the recipient gets the email, it's telling them this is an encrypted email. And sometimes you can set it so that it expires or you can set it so that they have to put in a password depending on what you're doing.

Gabrielle: So, the recipient knows and you could always send an unencrypted email saying, "Hey, I'm sending you an encrypted email." So that you know when you see it, that it's okay to open it up and then it will be unencrypted when the right person opens it. So, I don't know if that kind of helps us. Similar to when I use DocuSign as well, but we know there's lots of phishing emails that they try to impersonate DocuSign, is that I will usually tell whoever's going to get it that I'm sending you a DocuSign, a thing that needs to be signed, please look for it and open it.

Kirstin: That makes sense. That makes sense. Okay, well, we've got just one minute left. So, I don't know if we can answer any more questions during that time, but this has been so informative and I'm just like, oh, all the things that I'm not doing that I need to do-

Gabrielle: I'm not perfect either. Just so you know.

Kirstin: Yeah, yeah. But thank you so much, Gabrielle-

Gabrielle: You are welcome.

Kirstin: ... this has been so informative, and I'm so glad that you were able to be with us today.

Gabrielle: Well, thank you. It's been an honor to be here. And I hope that everybody got at least something out of this that they can use.

Kirstin: Yeah, thanks. We will talk to you soon.

Gabrielle: Okay, great. Thank you.