Cybersafety_ Exploring Safety Strategies for Cybersecurity

Tue, Jun 27, 2023 4:12PM 28:54

SUMMARY KEYWORDS

passwords, business, lauri, cybersecurity, pandemic, malware, technology, center, email, talked, consumers, work, information, ifas, opportunities, small businesses, people, hacker, phishing scams, podcast

SPEAKERS

Ricky Telg, Lauri Baker, Phillip Stokes

R Ricky Telg 00:04

This is Science by the Slice, a podcast from the University of Florida's Institute of Food and Agricultural Sciences Center for Public Issues Education. In this podcast, experts discuss the science of issues affecting our daily lives, reveal the motivations behind the decisions people make, and ultimately provide insight to solutions for our lives.

P Phillip Stokes 00:33

Welcome to Science by the Slice I'm Phillip Stokes, Education Coordinator with the PIE Center. It seems that the world has entered a new phase of digital dependence, software and systems are growing more complex, we are becoming more connected to each other through virtual spaces. And all of this can provide value to companies and consumers alike. In fact, what we're doing right now is an example of this in action. In essence, I'm talking to you through a digitally recorded audio file that was uploaded to a podcast hosting service. So people can then find it in a directory and listen to it on a podcast app, which might have been automatically downloaded to your device once the episode was published because you subscribe. By the way, please do subscribe. So all of that can happen because of how connected we are through the Internet. The Internet and the programs that rely on it are powerful, and with great power comes great responsibility. And that responsibility falls on all of us. As we engage in powerful internet-based activities, it's our responsibility to be vigilant of potential cyberattacks. So today's episode is all about the things you can do to protect your business or personal internet-connected systems from cyberattacks now, like today, measures you can take right away. And to share this with you, I'm joined by Dr. Lauri Baker, Associate Professor of Agricultural Communication at the University of Florida, and affiliate faculty member of the UF/IFAS PIE Center. Dr. Baker also co created the Center for Rural Enterprise Engagement or CREE a faculty driven interdisciplinary research center that serves as a generator and source of knowledge about new media marketing in an effort to enable rural and agriculture based businesses to flourish in ever changing environments. Dr. Baker and I discuss the importance of having a robust cybersecurity plan, educating yourself and your employees and investing in the right tools to protect your electronic data at home and at work. Well, Dr. Lauri Baker, thank you so much for being on the PIE Center's podcast Science by the Slice, of course, you know about the podcast pretty well as you are a an affiliated faculty member of the PIE Center. So I'm just want to give you a chance to introduce yourself and tell us a little bit more about who you are and your different research interests.

Lauri Baker 03:18

Yeah, great. Happy to be here. Thanks for having me. As you said, I am an affiliate faculty member with the PIE Center and my home department is in Agricultural Education and Communication. And when I came back to Florida as a faculty member in 2019, I brought with me a partner center to the PIE Center, the Center for Rural Enterprise Engagement. And so we work across multiple institutions at Kansas State University here at the University of Florida, as well as the University of Minnesota. And our goal really, is to help small businesses, particularly ag based businesses, use technology more efficiently to connect with consumers to sell products to consumers, and to engage in a positive way. So that really is the basis of a lot of my research and extension work.

Phillip Stokes 04:10

That's great. And, you know, I'm thinking about the different technologies and the different applications that are available to agribusinesses. And just small businesses in general that weren't around 10, 20, 30 years ago. I mean, it's pretty immense, how different it is, right? And so what are some of those technologies and those things that business owners have access to now?

Lauri Baker 04:34

Absolutely. The landscape is really, really changed in the last 10, in the last 20 years, as you noted, certainly, and one thing that has really pushed a lot of change related to technology was the pandemic. So there were certainly a lot of negatives that came out of it. And I know you focused on that some in this podcast previously. And we've certainly done a lot of research around that. But there also were some real positives, that came from that related to online selling, in particular, having the opportunity to sell directly to consumers. And many of them did that for the very first time. Some of them had been set up before. And actually, when we started the center in 2015, online selling was something we talked about a lot, as well as social media marketing and conducted research in that area. But many stakeholders weren't really interested at that time. But I guess we planted the seeds. And when the pandemic happened, we got a lot of phone calls saying, you remember when you were trying to get me to set up an online shop, and I wasn't that interested? Okay, so now I'd really like to know how to do that, and how to make that work. And some of our research in other areas where we looked at producers who were able to survive the pandemic, for the most part, those were people that were able to pivot fairly quickly into some other sales opportunity. And for many of them, that was a direct to consumer marketing opportunity. And so they, in some cases, actually saw greater sales than they'd had pre pandemic, and were able to connect more with consumers, all through this new technology, or new versions of the technology and new opportunities that came from a situation that wasn't necessarily that positive.

P Phillip Stokes 06:24

Yeah, I'm thinking about, there are always going to be some people who are kind of on the forefront of accepting some of these new technologies, adopting some of them. Most people unless you are really forced to, you might, you might wait until there's a circumstance that you really have to respond to, and that was the pandemic, right? As you said.

L Lauri Baker 06:43

Absolutely. And, and truthfully, pre pandemic, it may not have been the best business decision for many producers. But because people were staying home and they weren't headed to hotels and restaurants, many of our producers needed to come up with an alternative. And so there were a lot of factors that kind of happened. At the same time, consumers were also more willing to purchase things online, to purchase directly from consumers and had more time to investigate those things and explore what opportunities were available.

P Phillip Stokes 07:17

So as business owners, and just individuals are adopting some of these new technologies, and putting them into practice into with their business, things move at a quick pace. And so sometimes we're not always prepared for some of the consequences, some of the things that come along with that, potentially some of those negative things, as we talked about. So today, we're talking about cybersecurity, of course, and so. So why should business owners, and just everyday people who, you know, are connected online, why should we all be concerned about cybersecurity?

L Lauri Baker 07:54

Absolutely, there are certainly some inherent risks to any technology really, but particularly technology, where you may be collecting or sharing personal data. In places where you're purchasing a product online, or you're selling a product online, there's an exchange of information that happens in that process. Sometimes you may not be selling something directly or purchasing something directly, but you're still adding in your birthday when you create a social media account, or you're adding in some details about yourself or your children or there are security questions on your banking app that might lead to somebody finding more information out about you. And unfortunately, some people may not have positive intentions with using that information. So we do have to be careful during these times. And I think the more technology becomes just ubiquitous in our lives, and it's everywhere, we may start to get a little complacent. And with that can come some risks. And sometimes, small business owners or individuals may think, Well, I'm not really at risk, surely, they're going to attack a large company where they can get a lot more money. I don't really even have that much money in my business account or my personal account. So I probably am safe. Well, there certainly are people that are going to go for the biggest bang and try for the larger companies. But the truth is the larger companies likely have full time IT professionals that are working on their cybersecurity issues, they're much harder to get into. And so hacker might make a decision to choose to attack a lot of small businesses or individuals as opposed to a large one because unfortunately, many people are not protecting themselves.

P Phillip Stokes 09:53

Yeah for sure. And we were talking about this yesterday, right. You know, us working at UF you know, we have a whole IT team that might be looking into some of these things. If you are kind of out there by yourself, you don't have those those teammates, and those staff members maybe looking doing some of that work for you. So what should people be on the lookout for? What are the types of cybersecurity threats?

L Lauri Baker 10:17

Yeah, absolutely, we can kind of break down the two cybersecurity threats into two categories, really phishing or malware. And so phishing actually has been almost mainstream, there have been movies kind of focused on those kinds of issues. So people may be more aware of those. But phishing scams are essentially where someone sends you an email, a text, some form of communication, It can even be a telephone call, and tries to get your information from you. And through that, then they can use it in all sorts of different ways depending on what kind of information they have. So phishing scams like that have gotten more advanced. So it used to be we all kind of heard, well, somebody from Nigeria sends you an email that you send them a million dollars, and they'll send you back 2 million. Well, they've gotten a lot more advanced since then. And so things might come to your email for yourself or your employees. And it may look pretty legitimate, it may have the name of a company that you do use, but perhaps the extension is a little bit different. And so in general, through those phishing scams, they might be able to get your business information, they might be able to get through firewalls and get your customers information, depending on how advanced it is. The other category that we think about is malware, and malware can be attached to phishing scams, or it can come in a different way more directly. But essentially, that's when a hacker can get into your system, and launch some form of malware. And the viruses can do different types of things the same as biological viruses, right, they all have kind of a different intent. Some of them are simply just designed to mess with you and your organization and shut things down just for fun on the event of a hacker, but some of them can be more destructive, and can be designed to get into bank account information, and then sell that online or use that themselves in another way, or collect sensitive data and information, not only from you, but from your customers from all of your contacts on an individual level.

P Phillip Stokes 12:42

Lauri, phishing and malware have been around for a long time, you know, about as long as the internet has has been around. And, you know, I think things are the landscapes changing a little bit where it's well known some of the some of the hazards and some of the risks of being connected online and some of the attacks that people can receive. But of course, you know, businesses, a lot of times rely on this interconnected web to do just to do all the work that they

they can, what is like the pulse kind of the the American pulse are the pulse on cybersecurity threats and some of the new technologies that are now on the horizon and here such as AI and machine learning and such.

L Lauri Baker 13:28

Yeah, that's an excellent point. I think the longer something has been out, right, the more comfortable we get with it. And the more we start to think that, oh, well, maybe there aren't very many concerns anymore. I know what I'm looking for. I'm not going to click on any weird emails. And as you say, on an individual basis, maybe some people nationally, there's a big discussion of kind of unplugging and some people taking a conscious choice to move away from social media, to maybe not allow their children to have access to those things. But you're right, businesses may not be able to do that it doesn't necessarily make sense for them, particularly when consumers are asking for more opportunities, more point of sale options, quicker sales, easier sales, which all come with new technology and new software. And a national survey with a global market research firm recently looked at people's fears related to artificial intelligence. And while the overall concern was similar for artificial intelligence, as was cybersecurity and malware and data breaches, the level of concern was much higher for some of those artificial intelligence pieces. And I think in looking at that and seeking to kind of understand that I think some of it may be that fear of the unknown and similar the way we talked about online selling being a positive of the internet, there certainly are some other positives related to artificial intelligence. Our CREE group actually has a blog post on five different AI tools that you can use to help your business be more efficient. I was actually in a meeting yesterday and somebody said, well, I don't think we have to worry about ChatGPT replacing employees. But we might have to worry about an employee using ChatGPT, replacing employees who aren't using it. And so I think there will continue to be this balance of in order to be more successful, as an individual, as a business owner, within the United States, a very tech driven country, we're going to need to find ways to use technology, the most efficiently, the best that we can in order to continue to grow and develop our markets, and our abilities in many areas. Because if we are embracing them, we'll kind of get left behind the curve. But along the way, we really have to be diligent and paying attention to the cybersecurity issues that surround new technologies.

P Phillip Stokes 16:16

Yeah, absolutely. Yeah, we have to invest in these technologies to keep up but also we have to be aware of best practices around cybersecurity. And you you along with others have have made a list of some of those best practices. So I think we can just kind of go through some of them now. And for everyone listening, we can we can give you some of these tips that you can follow in your business or just in your your home life. So first off, Lauri, you've said to have a cybersecurity plan.

L Lauri Baker 16:48

Yes, absolutely. And I think it may seem kind of cheesy to some people, particularly if you're an individual thinking am I really going to develop a cybersecurity plan for my family. But you probably should be considering that. And if you're a small business owner, in particular, you absolutely have to have a cybersecurity plan. You wouldn't launch a new product without having a plan for it. You wouldn't make any other business decision without planning for it and managing it. So there are some tools to help you do that. The FCC, the Federal Communications Commission actually has tools and resources for small businesses in particular to help them develop a cybersecurity plan. But kind of within some of our best practices, you could walk through some of these and start these practices, even if you haven't developed a full on plan to make sure you're aware and paying attention to each piece that could affect you adversely.

Phillip Stokes 17:55

Yeah, it's all about preparing much much like preparing for, I don't know, a natural disaster. You always want to prepare during those times of blue skies when things are going just fine. Next, Lauri, you have educate yourself and your employees about cybersecurity.

Lauri Baker 18:12

Yes, setting up team meetings where you have this as a discussion item, a regular item that you're having conversations about, so much of it is just being aware of what's out there. So paying attention. Is there a new scam that's out there? Is there a new way they're attacking email? Another piece that certainly related to those conversations is your employees personal technology probably also needs to be updated. As new software comes available to them, they need to be doing those upgrades and having those conversations that they likely have access to your email on their phones, they're taking photos, maybe they're uploading things to social media for you. So it really has to be a team effort. It can't just be one person involved in cybersecurity.

Phillip Stokes 19:07

Well, and what you just said there about, you know, keeping things up to date kind of leads into the next point of getting anti malware software and keeping it updated.

Lauri Baker 19:17

Yes, yes. And those two have to go hand in hand. And honestly, I am the worst about not wanting to do updates. I keep thinking oh, well, after this next thing, all update because I don't want to shut down or I don't want to do this. But again, having those regular check ins and having that plan in place so that you're doing those things is really important. There are a lot of malware options or protection options out there. And we certainly don't advocate for any particular brand. Decide what works for you. It certainly depends on the size of your business and how many devices you have and what type of data you have. But the most important thing is having something in place that is regularly looking for what threats are on the horizon and protecting your devices. And key doing those updates to that protection along the way.

Phillip Stokes 20:09

Next, Lauri, you have store and backup your data using Cloud Storage. And I assume Cloud

Next, Lauri, you have store and backup your data using Cloud Storage. And I assume Cloud Storage is kind of a key part of that.

Lauri Baker 20:17

Yes, absolutely. That's a huge component of it. And I think more and more the cloud has become common language that people understand what that is. But they may not understand why that's so important versus storing something directly on your computer. There is something inherent to if it's on my computer, I own it. But if something happens to your computer, it could be a physical damage to your computer. But certainly, if you fall victim to a phishing or malware situation, it could destroy all of your data, it could ruin your machine, it could do a lot of different things. And one of the things that you really would want to make sure you've protected are any files that wouldn't be anywhere else, any things that you share with other people to make sure that you're storing those not on a physical device but in the cloud. Again, we don't like to make particular recommendations for which one, there are tons of options out there and available to you with different price points, and different sharing capabilities, whether you're a family or whether you're a small business, but some of the ones you might think about looking at, you know, Dropbox has options within that area, and lots of sharing opportunities. Microsoft also has some products that that fall into those categories that you may be able to add on to an email, Outlook kind of subscription. Google also has some options. So there are plenty of choices out there. But again, making sure that you have something that will store your data and important files somewhere other than your physical device.

Phillip Stokes 22:02

Lauri, the next one is something that every I'm sure everyone listening probably struggles with. It's our passwords, passwords matter. And I probably have about what 50 You know, so like, what advice can you give on passwords?

Lauri Baker 22:18

Yeah and passwords. You're right, we all get angry about having to change them. I suspect many people are reusing the same password over and over again, that maybe they created the very first time they had an email account. And I know we're all guilty of having some options that we do that with. But it's really important that you not do that repeating passwords can be one of the worst ways to fall victim to a type of scheme. Because if if a hacker is able to get your password in one place, and then you reuse that password that is on maybe your personal email, and you've used it on your bank account, and you've used it on your business login. Well now they have access to everything. So it's important to have different passwords. It's also important to have passwords that are not your birth date, or your phone number or easily guessable items. So having some of those stronger passwords that have multiple characters that may be sentence structures, numbers. Many systems have different requirements for passwords. And that is something that's becoming more standardized to require higher level passwords. But the repeating of passwords can certainly be a big challenge within that. The other piece is there have been more and more opportunities for small businesses and members of the public to have additional authentication. And so when that type of services available, you should take advantage of it. And that's simply something that maybe you enter your password, but they also require to send you a text and have a code that you enter so that you verify that it's you and there there are different formats of that and technology is continuing to emerge in those areas. But anytime there's an offer for something even better than a password as a backup, you should try to take advantage of that.

P Phillip Stokes 24:25

Okay, Lauri, the last one, the last tip you have is protect your data.

L Lauri Baker 24:31

Yes, absolutely. One of the things that, particularly in a small business we do is maybe we sign up and we only have one design account, and then we share that password. Again, not supposed to be sharing that password but we share that password with everyone within the whole system or we store it in a place where everyone can get it. Well you certainly trust all of the people that are around you. But if people don't really need access to perhaps customers, phone numbers and addresses, it's not something that's a part of their job. It's somebody, maybe in your family that's helping you take photos on the farm. Well, if they aren't emailing those photos or sending them directly to customers, then they probably don't need direct access to customer information. And I know there is a tendency to want to be transparent and share with everyone. And those are good goals and things that help a business function, but also understanding what people really need to know and what people don't need to know. So protecting your data internally, and making sure only the people that really need data have access to that data, and that it does have all of the passwords protected and all of the other best practices that we've talked about around it. But that includes managing your kind of internal audience as well, the same way that I don't give my 11 year old my credit card number. I instead, if he needs to purchase something, I go over to his iPad and use my finger authentication to purchase something instead of directly giving him that information.

P Phillip Stokes 26:17

Yeah, that's wonderful. And that, that those are, you know, all the tips that we have. And I should say this, I do want to say this, the everything that we've talked about, we have a publication on that, we'll include that in the show notes. So if you're listening, and you want to go back and refer to these and get some more details on that, we'll list that in the show notes. Check it out there. We'll also have some other resources. You know, as we're kind of wrapping up here, Lauri, I guess I couldn't help but thinking like, if our like grandparents, or great grandparents heard us talking right now, they would think we were like, in a in a futuristic sci fi movie or something, you know, like, I guess I'm just thinking, like, the future is here, and we are living in it. And all of those things that that may have seemed like a dream before. I mean, they're they're upon us. And so yeah, it's in some ways, it's kind of scary. In some ways it's, it's really great because it, it does help us have a higher quality of life, and be able to do more and be more connected with our friends and our family. But that comes with some things that we need to account for.

L Lauri Baker 27:24

Right. Absolutely. And yeah, we can't say that we would turn it all off. I don't think there are just too many benefits and too many opportunities, particularly in agriculture, where we're trying to feed the world, right? We can't do that without some of these advanced technologies. So it is important to just stay vigilant. Pay attention. Don't be overly scared, but always be prepared.

Phillip Stokes 27:48

Sure, sure. Well, wonderful. Well, once again, such an important topic and Dr. Lauri Baker, I want to thank you for being on Science by the Slice. And I'm sure we'll have you back here real soon.

Lauri Baker 27:59

Okay, thanks enjoyed it.

Ricky Telg 28:03

Science by the Slice is produced by the UF/IFAS Center for Public Issues Education in Agriculture and Natural Resources. Thanks for listening to today's episode. Subscribe to Science by the Slice on your favorite podcast app and give us a rating or review as well. Have a question or comment? Send us an email to piecenter@ifas.ufl.edu. That's piecenter, all one word, at ifas, I-F-A-S, dot ufl dot edu. We'd love to hear from you. If you enjoyed today's episode, consider sharing with a friend or colleague. Until next time, thanks for listening to Science by the Slice.