**Eye on Security**

**Tackling Digital Safety for Women**

**Transcript**

Luke McNamara:

Welcome to another episode of the Eye on Security Podcast. I'm your host, Luke McNamara. And joining me today to talk about digital safety for women, a lot of the content coming from a talk that they had recently given for the Grace Hopper Celebration is Cris Kittner, principal analyst here at Mandiant Threat Intelligence and Lillian Teng, director of Threat Investigations at Verizon Media. Cris and Lillian, great to have you here today.

Cris Kittner:

Thank you for having us.

Lillian Teng:

Thanks for having us.

Luke McNamara:

So, we're going to get into some of the advice and the content of the presentation that you guys put together, but I first wanted to hear a little bit about the background for this talk and sort of framing the problem as you see it with respect to digital safety for women. Cris, maybe we can start with you.

Cris Kittner:

Sure. So for me, the background of how I started this was I originally did presentations for kids' schools for tweens and teens about how they could be safe on the internet, with a specific focus of the nudes that are shared and who actually gets in trouble at school for that kind of thing. It typically means that the victim and the perpetrator of some sort of sexual harassment that's done on a social media or device, they both get expelled. So that was part of, "Hey, let's talk about this and teach these kids how to be safe on the internet and focus on the girls who were victims and are now also being expelled." And from that, obviously there's a need as well to normalize that conversation as we get older. And that's how I kind of connected with Lillian who had the original idea for this specific topic.

Luke McNamara:

And Lilian, this is a big piece of what you focus on in your day-to-day job at Verizon, correct?

Lillian Teng:

Correct. So the organization that I lead, we focus on protecting our consumers from malicious actors on the internet. One of the reasons why I'm particularly passionate about this topic is that women are disproportionately affected by cyber crime. Now that we are online almost all the time due to COVID, things are amplified. So things like cyber stalking, cyber bullying, cyber harassment, image-based sexual abuse. These are things that disproportionately affect women. Also, like as folks are voicing concerns in their communities and folks have opposing views, digital safety is becoming more and more important for people. One of the things that weighs heavily on my mind is again, women have been the predominant targets like Cris had mentioned, of image-based sexual abuse. You can hear this referred to as like a revenge porn or non-consensual pornography. We try not to use the term pornography. Pornography is legal.

This is image based sexual assault because you are committing an abuse against somebody who's not consenting to this activity. According to a poll conducted by Amnesty International in 2017, 33% of the female respondents experienced some form of online abuse or harassment. That's a lot of people. Of all those women who were surveyed, who reported this type of harassment, 41% of them said, at least on one occasion, they felt that the online experience had transitioned to the physical world. So they were threatened with actions such as doxing or unauthorized sharing of personal information. The psychological impact of this abuse is devastating. Again, this survey was conducted by Amnesty International, but it said 61% of those who said they'd experienced this online abuse, experienced lower self-esteem or loss of confidence. More than half of the responses said they'd experienced stress, anxiety or panic attacks after experiencing online abuse or harassment.

And 63% said it actually affected the quality of their sleep. And as we all know, sleep is incredibly valuable for mental health. And especially in stressful times. One of the other factors that I would like to cite actually is women are underrepresented in the cyber security field. Depending on which statistic you look at in technology jobs, women are represented at maybe like 20 to 30% and in the cyber security field is even less than that. So it's maybe 10 to 20% if you're being really optimistic. And so it means that these problems are not being bubbled up because we're not being represented in the communities that need to address these problems. So that was another reason why I wanted to reach out to Cris, who is our partner. And then we had another partner, Brittany Barbehenn from Palo Alto Networks who collaborated on this talk with us because we are three women in cybersecurity. And we wanted to use our voice to help protect others.

Luke McNamara:

And a lot of the advice and the content in your presentation, that's drawn from your experiences working in cybersecurity. Cris, you work on the cyber espionage team here, and you have these perspectives of seeing some of the activities and capabilities of a range of different threat actors carrying out operations in this space. But one that maybe doesn't always in terms of the best practices around some of the things you talk about here, some of those techniques and methods for staying safe online are things that necessarily bubble down to end users. The audience, particularly that you were giving this talk to, was this primarily people that worked in security or tech? Or what was the sort of background they had that you were going in to talk to?

Cris Kittner:

So the first two times that we presented on this, they are young women entering in the field of

computing and IT, to some level. And again, as Lillian said, it's that underrepresented women in these fields. So if we who have been in the fields for a while, and I can say this myself and I'm sure others will say the same thing, we've all experienced both sexual harassment in the physical world, but online. Whether it's through conferences that exist or interactions with other people in the field, but most people have experienced it. And being able to, as a “growner” grown-up tell these young women, "Hey, this isn't right. It's not to be expected. We have experienced this. We are going to tell you and help you, so you don't have to go through with it because there is the very huge stigma that is associated with being a victim and then having to come forth." And I feel very strongly that it is important for us to teach the younger kids, as well as young women who are entering the workforce that, "No, this is not expected."

Luke McNamara:

And one of the things that you're highlighting there, Cris and Lillian mentioned as well at the beginning is how this is particularly an issue where it's not just something that exists in the cyber realm, but there's often like a very close relationship between activity and behavior that's taking place in physical spaces, as well as online. That seems to be a key component in this message that you're pushing.

Lillian Teng:

Yeah, I would definitely agree. Again, I think with regards to the connection between real-world harassment and cyber harassment, it goes both ways. So for example, in the United States, one out of every 12 women, so about 8.2 million women in one out of 45 men. So about 2 million men have been stalked at some point in their lives. And one in four of these reported stalking victims have reported that some form of cyber-stalking, so email stalking or instant message stalking has occurred. So that kind of shows how society now we rely on technology and so it bleeds into these real-world actions.

Luke McNamara:

So I want to get into a little bit of some of the advice that you give here in this presentation and touch on some of the things that you recommend. So when people are thinking about this topic of digital safety, there's a couple key areas you seem to highlight. Can you go into and explain a little bit about what those are?

Lillian Teng:

Yeah, sure thing. So the one thing that I think most people talk about is this concept of what's called password hygiene. And so that's making sure that your password are number one, piece of advice is do not reuse your password across multiple sites. Once one site is compromised and a malicious actor may have your password, they 100% will try it against all of your other websites. And so you need to have unique passwords for every single login that you have. Yes, I know that's cumbersome, but one of the ways you can resolve that or mitigate that is to use something called a password manager. There's lots of them out there. Lots of them are free. And there are some that are paid that have great features, cloud backups, things like that. So we strongly recommend that you use a password manager.

Well, the other thing to consider, and this is actually built into a lot of password managers, is this question of complexity versus link. There are a lot of websites out there that say your password has to have like a bajillion special characters. You have to pat your head and rub your belly. And Jupiter has

to be in alignment with Saturn for you to set this password. And one of the things that we try to focus on for a lot of people is that sometimes it doesn't really have to be that complex. Sometimes length is just going to get you where you want to be, just with average computing power, the way it is. If you have a 16 to 20 character password, that is going to be cumbersome enough for a bad person on the internet to give up on trying to crack your password and move on to somebody else.

Lillian Teng:

And so it's not the greatest feeling, but you don't have to be the fastest. You just can't be the slowest. So-

Cris Kittner:

We had a visual that we showed during the presentation that really gives an example of a good 16 to 20 character password versus a bad one.

Lillian Teng:

Yeah. One of the things you have to consider too, is like, it's impossible to remember so many passwords. And one of the easy ways to overcome that is well, it's just to use a passphrase. So I believe the example I used in the presentation was cookies are delicious or something like that because it has enough characters to get you where you want to be in terms of length. And if somebody requires that password to be complex, you can remember the phrase and then just add the complexity as you need it. But it's easy to remember and we'll hopefully mitigate some of the attacks adversaries. The interesting thing also is that people complain about having longer and complex passwords. A lot of kids nowadays during the pandemic, as young as kindergartens, remember complex passwords. My own kids have passwords that are different for several of their applications. And they remember without a password manager, which I don't know how, but maybe generational it is possible to do it and be safe. It just takes time and effort.

Luke McNamara:

Well, that's an excellent point too, that if you have a system that is usable, that you can remember, that you will actually implement on your different devices. That often is a much better solution than an incredibly complex and sophisticated means that you don't use. There's probably a principle that's true in a lot of different areas of security.

Lillian Teng:

Yeah. Honestly, it's just balancing, it's knowing yourself and knowing what you're going to be able to use. Like if you know, yes, I am super great at remembering all of these widgets that go into my password, then go forth and do that. But if you're a person where you know that may not be realistic for you again, try using a passphrase and just make it longer.

Luke McNamara:

So what are some of these other areas you get into, account security, social media, obviously the importance of credentials and having secure credentials and keeping those secure is something I would

imagine would also be applicable to those areas. But what are some of the things that you get into when you talk those areas?

Lillian Teng:

One of the things to consider is the security of your device as well. So there are a couple of factors that play here. So if you are using a pin for your phone, obviously longer is going to be better. You don't want to use like five ones as your password. You do want to make it something somewhat robust there. You also don't again, want to reuse your pin. Don't use your bank pin. Don't use anything that is a personal identifier. So don't use your address number. Don't use your zip code. Don't use your birthday. Cris, we'll talk about this a little bit in the social media section, but you see all these surveys that go around social media that are like, "Your superhero name is the street you lived on and your mother's maiden name."

Cris Kittner:

Don't do that.

Lillian Teng:

Well, one of the things that a lot of people don't realize is those are the security questions to get into your account. So you should not be doing that. We actually saw one recently, that was pretty hilarious, that was, "If your social security number or how much money you had in the bank, how much would that be?" And a lot of people actually were posting their social security numbers.

Luke McNamara:

Oh, no.

Lillian Teng:

And so be careful what you share on social media, because the adversaries are out there and they want to make it fun and they want to engage you. And this is how they're collecting this kind of information. So going back to your security settings, people might say, "Well, fine. I'm just going to use biometrics." Which is a great option. You can use facial recognition, you can use fingerprints as well. But one thing to also consider with that, and especially with a lot of the social and racial injustice that has happened. And a lot of the protests that are occurring is that when you were out and about in the world, if you anticipate potentially having interactions with law enforcement, one thing you may want to consider is either using a pin in those particular cases, because there is a concept of search and seizure.

If you use a pin, law enforcement can't compel you to disclose something you know. That being said, if you're using facial recognition or a fingerprint, they can compel something you are. So that's always something to keep in mind. And there's a lot of information about this from various non-profits who are working with these types of organizations to keep everyone safe. So things like the EFF, the Electronic Freedom-

Luke McNamara:

Freedom Foundation.

Cris Kittner:

Freedom Foundation.

Lillian Teng:

... Freedom Foundation. Yeah. So they have a lot of really great guides. So I would highly recommend checking those out. Other things again, along the same vein, people love to check in, do your Yelp or check in at specific locations, but that also gives folks an insight into where you are. And so if you check in at a restaurant, people can guess, "Oh, I'm not going to be home for the next hour." And that could have real world consequences of people knowing you're not going to be in your house for an hour. So strongly advise taking a look at your GPS location data and where you're sharing it and if you feel comfortable sharing it, because some people they're fine with that. The other thing, as well, as to be aware of scams, like we basically live on devices these days. We live on phones, be aware of things like smishing, SMS phishing. People masquerading as a contact and asking you to click on a link. So do be wary of that.

Luke McNamara:

Yeah. I was going to ask you some more about the location services or just that sort of component of security. So as you mentioned, there's ways in which the devices that we use either purposely, we may put out our location because of an app or system we're using. But also just in general, there may be leaking location data that we may not be aware of. There's also, of course, if you're on social media, maybe you're posting images that either you're specifically tagging to a location or that there's location data included in that. How should people be thinking about this as another sort of component of security?

Lillian Teng:

No. That's a great question. And we're not going to give you like a, "You must do this or you must do that." Because we recognize that everybody's situation is different, but it's just being cognizant of some of the things that you brought up. So being cognizant of which applications are using your location data. Like, do you want social media like Facebook, Instagram, Twitter, knowing your location? I mean, that's up to you to decide. Would you want Google Maps knowing your location? Yeah, probably. That probably makes a little bit of sense, but if you have a calculator app or something like that, I would maybe be a little skeptical about giving that my location service. And so it's just about going through checking your apps and making sure that the permissions they're asking for are appropriate. That being said, it is easier said than done because there are a lot of app developers out there who just ask for the keys to the kingdom.

Lillian Teng:

And then at that point, it's just you assessing your own risk tolerance. Cris, do you have any comments? Because I know you have some feelings about those with

Cris Kittner:

I do.

Lillian Teng:

... social media.

Cris Kittner:

It's interesting because a lot of the different topics that we discuss in our conversation focuses on how to be safe and like simple things that we can maybe do now to ensure our safety. And they also all kind of overlap. So in terms of pictures and geolocation, as Lillian mentioned, for example, not a lot of people know that a video that you take on your iPhone or a picture may include everything someone needs to know where you were when you took that picture, the day, time, location, all of it. So if you then share that picture, even if you didn't necessarily say where you were, the information is there. People just don't think about that.

Similarly, if you have certain apps like you want Google Maps to know your location, or maybe not. But you do, if you're driving somewhere. Think about whether you're going to choose under settings to always share your location or never, or make sure it asks or only when in news. That's kind of important tidbits that everybody should do. Similarly, it's impossible to know off the top of your head, how to change and adjust the privacy and security settings on the 453 social media apps that we use nowadays. For example, the most commonly used, and I won't go into names, but they have between five. I think the last one I checked was 21 steps that you have to click and toggle in order to get to what you feel comfortable with. And to me, that's astonishing. Why do we have to tell them, "Don't share all of this that you shouldn't share anyway." It's our information.

So knowing how to check that should be remembered by everyone. There's also the idea of third party applications. So a lot of the social media apps that we use connect to other accounts that you may have. What permissions are you giving? Do you even know how many accounts you have that share your Google or Facebook or whatever password? There's so many things and we did have cool handouts that had specific things that you can do. Perhaps we can share with you Luke, another time and you can share with others. But if you take the time and you sit down and you go through, it is possible to maintain the level of safety that you want on the apps that are not my recommendation personally, it's just don't use it if you can help it.

Luke McNamara:

That's an important point, I think you're making is that a lot of this is awareness around what is your current sort of risk tolerance? Are you aware of the different tools or settings, the sites that you're using and the sort of data that you may be leaking out unintentionally?

Cris Kittner:

And the other important thing that I should mention is the terms of service for each of these websites or apps. It's really important to read it if you want to know what that company is going to be able to do with your information on the stuff they're collecting. It depends on what kind of company it is, what country it's headquartered in. So the laws differ and most people don't really read that. The statistics are

something like maybe 40% of people start reading them, but never finish. I try to read some, if I can't finish it, I usually just don't do it.

Luke McNamara:

Yeah. And I think it's a lot of us.

Cris Kittner:

They don’t do it. Right.

Lillian Teng:

So one thing I do want to emphasize that you brought up Luke here is our assistance of data. So one thing that I think a lot of people forget is literally nothing dies on the internet and nothing dies when you put it on a computer. I started my career in cyber forensics and it's amazing the types of things you can recover for our computer. And so chores again, Cris's point about teaching young people, the implications of doing some of these actions. One of the things that we probably should emphasize a little bit more is like, you should be intentional because while you think, "Oh, I can take the snap and I can just delete it, it doesn't die." It could go up to a cloud server and be resident there somewhere. It's still resident on your device and if somebody wants to pull it, they can recover it.

Lillian Teng:

Like, just be thoughtful about the types of things you want to put into digital media. When I was growing up, you know, obviously dating myself. This wasn't necessarily as much as a concern because you would literally have to take a picture with a camera, get it on film and have it delivered or developed. But nowadays you just click it on whatever device you're on and it's there and who knows how to get rid of it, honestly.

Luke McNamara:

Well, that's an interesting point too, that maybe we can circle into talking about the sort of feedback and response that you've gotten from this. Because I'm curious, Cris, you mentioned doing some of this work with children. Is there some of these areas where younger individuals that have maybe more familiarity with some of these emerging technologies, do you find that they are more aware of some of these different ways in which data can leak out or things that they know they need to be secure of or the persistence of data? Are there some areas where that there is an advantage because they're growing up with technologies that maybe they're not thinking from a security minded standpoint, but they grasp some things more intuitively?

Cris Kittner:

That is a fascinating question because initially I thought, "Yes, that will happen." And that's the case. I don't find that at all. Kids are still kids and their development age does not allow them to logistically make decisions about whether or not to share their selfie or nude with someone. When I explained that Snapchat, you could take a screenshot of the picture, there were several people that were very surprised about that. And the fact that they just don't think doesn't mean that they're not good with

technology. It just means they're kids. Now I have also heard from grown women and men that didn't think, and then sent. My own personal philosophy is I won't have anything that I would be humiliated were to be shared. But again, kids don't get to that. I think it's really important more than anything is to get to the bottom of where the problem begins.

Having kids understand how people should be treated, both men and women. And that's where it starts. I really wanted to bring awareness to these kids. And especially girls, I'll be honest because I've always been very open with my kids. And I see the activity that they have going on, on their iPads or phones. And I'm that mom, the one that will call the other parents with concern. It's not very welcome all the time at all, but thankfully I have found that my own kids and some of their friends will come to me when they have an issue like that. So I look at that as a small win. Similarly, I have a handful of anecdotes where young women who either started at the cyber security industry where some women legitimately did not disclose sexual harassment or assault because they kind of thought it was just par for the course.

So with that in mind, I find that it's very important to let everybody know, "Hey, let's normalize this conversation. This is not acceptable in high school or in your career. And let's eliminate the stigma and make this a conversation that everybody can have to give kids and older adults that power." So an interesting antidote actually with regards to impact on young people and do they embrace security a little bit more quickly? I think they are inclined to do it if we talk to them about it and tell them about the consequences. So, one thing that actually happened when Cris and Brittany and I, we did a dry run of this talk for one of the employee resource groups at Verizon Media. And one of the attendees actually texted me during the talk and said, when you were giving your discussion of password hygiene, my daughter actually put us on mute and said, "Mom, my password is not secure enough. I'm going to go change it now."

So again, it's about providing the information, providing the tools, letting folks evaluate to themselves, "Is this important? Is this not important?" And then being able to take action based on that information. So, that is definitely a positive outcome that came from one of our trial runs. Some other feedback that we've gotten, obviously it has been very well received and we'll support it. But one of the things that is disheartening for us is there are a lot of women who did say that, "Hey, I am experiencing harassment and can you help me remediate this in some way. Somebody has created a fake social media profile that is impersonating me." Things like that. And so, one of the recommendations that we have there again is to just be careful, like, what do you post on social media?

Cris Kittner:

Can it be reused? Can somebody else grab it and use it and try and impersonate you? One of the things that we do recommend is obviously if you are a victim of this reported to the service, most of the social media services have trust and safety teams and abuse lines that work tirelessly to help their users. And so that's something that I would just encourage everyone, just go look it up and go report it to the correct team at that point. But it was for us great to receive that positive feedback. The fact that even though folks are aware of the technology, giving them that enhanced knowledge on how to protect themselves when they're using this technology was beneficial. I also found really interesting that although we created an email alias for the audience to talk to us directly, should they have further questions, I personally, and I'm not sure if it's based on what we discussed, but I, during the presentations focused a lot on the harassment and image-based abuse.

And I had a lot of people reach out to me, not with that alias that we announced, but either through Twitter or LinkedIn, some of them to share their own stories. And thank me and others to ask for more resources or just say, "That was great. Thank you." It was on LinkedIn and ... Yeah. Both of those. I had a few men that also reached out and were interested in having heard that point of view. So honestly, when I think about this and I think what are the main things that I would like to be the impact of this presentation, I think that as people and users on the internet, we should definitely be aware of our surroundings because nothing ever dies on the internet. That focus on normalizing the discussion and removing stigma for the victims is paramount and really supporting women and victims so that they are empowered and also feel empowered by others.

Luke McNamara:

In the feedback you received, were there any aspects that you were somewhat surprised by? I don't know if there's any particular areas that you covered, that maybe some things like password hygiene, that if you work in security or work in tech, maybe you're more familiar with. But were there other aspects where people reached out and were like, "Oh, I hadn't really thought about the sort of security area around this or how this is a potential privacy area."

Lillian Teng:

I feel like I've been giving security talks all throughout my career. So nothing surprises me these days.

Cris Kittner:

I'll say that too, because some of the stories that I got shared with me were out of this world absurd, but I was not surprised.

Luke McNamara:

Well, so it's a bit of a leading question because one area where I've seen some discussion around is with the increased popularity around messaging apps, secure end to end encrypted messaging apps. And just the reminder needing to be pushed, that while the communications from point to point are secure the end points of those, the device that you're using, you still have to think about that. So as you were talking about these different areas of security, I think giving people a sort of holistic view that it's important, that they all work together seamlessly that you can't just focus at one area on the expense of another. That seems to be an area where there's people that use technology. Sometimes we're not as good of thinking. And where I think having that sort of adversarial mindset that I'm sure you both have to have in your day jobs of thinking through how an adversary would look at that you have that, but do you see that being a challenge for some people to not necessarily know how to put all these things together and practice?

Lillian Teng:

So I think with regards to our talk, like we tried to just hit kind of the foundational areas. And so you can build upon maybe integrating a lot of these things. Honestly, I'll be happy if you take one step at this point and then master it and then take another step. Our talk was... How long was it, Cris? An hour, 90 minutes.

Cris Kittner:

It was an hour-

Lillian Teng:

Yeah.

Cris Kittner:

Interactive exercises that are very helpful. We can tell you where to go and try it, but I'll let Lillian get into that.

Lillian Teng:

Yeah. So honestly, it was a jam packed hour. And so we could not cover everything that we want to cover. I think kind of to your question, Luke, like that is probably a little bit more advanced than what we're trying to achieve here because a lot of people just didn't even have baseline knowledge of some of these security features.

Yeah. One thing I realize we didn't actually chat about with things like account security. We provided some tips on how to secure just your generic accounts, your email accounts, your social media accounts, specifically focused on email, which is what most people use these days to communicate. They're things like checking your filter settings, people block certain spammy emails that they may get. But one of the things that a lot of folks don't think about is you should check these because of a malicious actor has gotten into your account. They could potentially be filtering out emails from your service provider, trying to communicate to you that there might be a security issue. They do that intentionally. Another thing that we advise people as regards to mail forwarding, check, if your mail is being forwarded somewhere you don't intend it to be forwarded to. Because that happens as well.

I think, our colleague Brittany shared a story of someone she knew whose device to your point, Luke had been compromised. And one of the things that had occurred on the device was that they were forwarding email and the user was not aware of it. And so personal communications like, "We're going to meet for lunch at here," and the things like that were going to somebody that they did not want to be communicating with, or did not want that person to know where their whereabouts were, were tracking them, because they had enabled this function. Other things to also worry about, application specific passwords. This is where you connect a device to like a service of, for example, putting a particular mail service on your mobile device. Oftentimes, you need to have something called an application specific password to do so, but that being said, malicious adversaries can get in there and create fake applications' specific passwords that mimic things like Yahoo Mail, Apple Mail, Google Mail, Hotmail, things like that.

And so you think they're legitimate, but if you don't recall actually doing it, you may want to go and check and see if that's something that is persistent, because if you change your actual email password, that application specific password could potentially also bypass that. So just things that I don't think folks are necessarily aware of that they've done these, just giving them the knowledge so they can think about it, decide if they want to use it. Undo them, if they decide that this is a risk that don't want to take. That was kind of what we were focusing on. But thank you for that idea, Luke, maybe we'll do that as a follow-up to a Grace Hopper in 2021.

Luke McNamara:

Well, so, that's a great transition, I guess, to final thoughts and comments here at the end with, obviously this seems like a talk that you provide a lot of women with a great set of resources to think about. Areas of secure to think about, but then also highlighting this as a problem. Any sort of additional thoughts on this and things that you feel like are whether you guys are going to do those in a follow on presentation, or you feel like they need to be focused on more areas that could kind of fall into that category?

Cris Kittner:

I don't think that I would be the right person to address the questions that I have, that have emerged or remain from studying this topic so far. But I would be curious to know how do we address it, not just on an individual incident basis or in a particular school or work environment, but how do we address it in society? Because it starts down there and that's some sort of psychological or other development research that I don't have the means to do, but I wonder, could that result in changes to what we see as these kids get older and become men and women?

Lillian Teng:

I would echo Cris's point. I think one of the reasons that this topic is important is again to normalize conversations. Yes, this happens. Yes, this is prevalent. Yes, it has not been talked about. And it hasn't been talked about for a couple of reasons. It is an uncomfortable subject. And again, like I'm in an earlier in the interview, these perspectives are not necessarily represented in the community. And so elevating that, getting more people on board, getting more people to think about it, getting more people to ask these questions-

Cris Kittner:

And speak up.

Lillian Teng:

... I think. Yeah. And speak up, is really a great, additional benefit to doing these talks.

Luke McNamara:

Well, Lillian, Cris, great to talk with you and thank you for the work you have done on this. I'm sure we'll continue to do. For folks who want to check out more of this, can they go and find resources around this? Are those available?

Lillian Teng:

So we had some resources for the Grace Hopper Talk. We don't host them publicly anywhere, but one some resources I would probably check out, I alluded to one of them earlier, which is EFF, has a lot of resources on cybersecurity and individual protections.

Lillian Teng:

I would just-

Cris Kittner:

... national, has great information on research as well.

Lillian Teng:

Yeah. There are a lot of great nonprofits doing work in this space. Citizen Lab is another one that does a lot of great cybersecurity research. I think just having these conversations and asking these questions, there's common sense. Media is another one. That's a great resource for parents.

Cris Kittner:

I use it often.

Lillian Teng:

Yeah. There's a lot out there, but again, kind of just thinking, assessing your risk, being skeptical.

Luke McNamara:

All good points to end it on. Thank you again for taking the time to do this and hopefully this will serve as a good resource as well for people looking to get started on some of the basics that you highlighted here.

Lillian Teng:

Thank you so much, Luke.

Cris Kittner:

Thank you for having me.

Luke McNamara:

Take care.