(00:01):

So, hi, I'm max. I responded to a tabs message that said, who's gonna hold the tab star workshop to clean up your shit, to prevent getting docks so that you can go out and do things that must be done in the world. I have, I'm just gonna dive into it. This is what I'm do. I'm gonna just dive in. It's been a while since I've done this thing, I am really nervous to be honest. So I'll just put that up front. And let's see. So my goal is to sort of run through some core material for you all. Jump in, ask questions, use your voice, cuz I don't have any idea how I would see if you tried to raise a hand. And for anybody who finds it useful to have voice and visual at the same time, there's no slides.

(00:56):

But I am pass pasting like the core concepts into the thread in the tabs channel and thread is tab stores, workshop on cleaning up your shit to prevent getting ducked. So I'm gonna start with some credentialing and literally the entirety of my credentialing this morning, evening afternoon will be, why should you trust me? Well, you really fucking shouldn't <laugh> I am hoping to present some material to you that is industry standard in a way that makes sense, that feels comfortable, that is accessible for you, but there's literally nothing special about me. There's no particular reason why you should think that I am an ex. The one caveat that I will give you is because the world that we live in, when you hear my female voice, you might be inclined to just like whether you want to or mean to or not to be like, ah, is she really technical?

(01:53):

And if you find yourself getting a little voice like that in your head try and nudge it to the other side, to recognize that I have been a woman on the internet since the DARPA days. And for me learning the fundamentals of information and threat management was never a hobby. It was purely survival. So I have learned this stuff because I had to not because I ever wanted to. So that's the credentialing step. Let me give you a quick summary of what we are gonna try and do here. So what I wanna do is run you through some real safe basics, the things that are useful for anyone. I started building these with some expert friends Ooh, maybe five or six years ago. And we've like modified the order of them from time to time, but it's been remarkable how steady and consistent and stable they have been.

(02:53):

So I'm just gonna run through those at a high level. I'm not gonna try and teach you how to do each of them, but I'm gonna kind of mark the core things that anyone who touches technology should probably be starting to do. Second thing I'm gonna do is really talk about what does it mean to feel safe. And that is often referred to as identifying what your threat model is. A threat model is really unique to an individual or an organization or company and threat model. Is this really like industry standard term? That sounds kind of scary. All it is, is sort of like looking at yourself, looking around you and making some prioritization decisions about what you wanna do so that you can feel safe so that you can go have the life you wanna have. And then I'm gonna talk a little bit about how you might apply this to your specific situation. And then hopefully I'll leave you tons and tons of time to ask questions. I know we have a couple of experts on the call today. There are many voices other than mine that can provide really thoughtful advice. And we may decide to stop the recording when we get to Q and a. So that's it. Any questions just about the coverage or the format or anything like that before I, I move into the material?

(04:16):

No. Sounds great.

(04:18):

Cool. All right. So, oh, the one thing that I did not say out loud, which is this is not this session is not specifically about preventing getting docks. Some of you are already fucking docks, like rusty, rusty is long since docks. The, the core of the intent here is to really think about what you have, what you're gonna do and how you can make yourself feel safe as you go out to do the things that you're gonna do. All right. You will also note that I'm, handwaving about some of those things that you might go out and do, I am going to intentionally hand wave about some of those things that you might go out and do. All right. So let's start with the safe basics and these are fundamentally the things that are good for everyone to do if they are on the internet in 2022.

(05:13):

So right up on the bot right across the bottom of everything is one core basic, which is if you have some things that are digital information photos leases, I don't even know if mortgage documents are electronic. Maybe they are, but anything that you have that if you lose it in a flood, a fire to children, rampaging through closets or the thing that we are most concerned about from the info sex space to ransomware, make yourself a safe, offline BA backup. My favorite backup is printing shit out <laugh> but there are lots of other alternatives, like grab yourself a quick side, hard drive make a cloud backup, just put something someplace else. One of the things that's a little weird about 2022 is individual human beings are getting struck by ransomware now at a really high level of ransomware is somebody figures out how to get to your disc.

(06:15):

They encrypt it, they drop you a file or a photo that says I can't believe this is still true. Give us your Bitcoin in order to get the DEC description key. And you pay the ransom. They hopefully give you the dection key. And then you get your stuff back. This used to be like only large companies. Then it was sort of medium companies. Now it's pretty universal. As soon as nation state actors or thieves or criminal organizations figure out that there is something that can make them some money, they just turn the hose on and pull some money outta those things. So a number one, think about the things that you wanna protect against flood fire, children who ransomware and take some steps to protect them against those things.

(07:04):

Second really big thing that if you are not doing it are ready, start doing it soon. So get yourself a password manager. Still today, one of the most frequent compromises people experience is a password that they used in one account that they long since forgot about, happens to be the password that they used someplace else, that account they forgot they even had gets popped. And then it's called credential stuffing. That actor is run around trying to just like log in as you to a thousand things on the internet. This is a little bit old, but there's this wonderful site from I think his name is Troy hunter called have I been PED and mostly a reliable actor. You should not be too terrified to like put your email address in here, but this will pull up a list of all of the compromises that your email address and password have appeared in. And so if you would like to sort of frame yourself a little bit, put your email in, find out which of your passwords are already in the wild.

(08:10):

The reason that we use password managers to mitigate this particular threat is because what you really wanna do is have a unique and difficult password for every single account that you log into. High quality

password managers, then protect those individual pass. You have one password that you memorize and hopefully some multifactor authentication that you apply to your password manager. And then if one of your accounts gets compromised, not all of your accounts get compromised. You don't have to try and memorize every single password that you have. Humans are bad at that. Computers are good at that. There are, I will just pause and say the clear caveat, like not everybody needs a password manager.

(09:03):

I figure most people on this discord probably need a password manager. But there are totally valid cases for like older people who just have like four or five accounts to like literally use a book, write it down, like randomize some words out of a book. So, but probably speaking most people, probably a good idea, go get yourself a password manager and start using it reliably. One of the other nice things is it makes it, it, once you have your passwords under password management, it makes it much easier to change them and rotate them. And so if something happens where you like, something just feels queasy. It is a much lower effort activity to go in and just like change every freaking password you have by using the mechanisms in the password manager then the next piece up the, the pyramid of basic internet security needs is multifactor authentication.

(10:06):

So this takes the form of you log in with your username and password. And then the, the system sends you a text message or you integrate your account with something like Google authenticator or athe or any number of other, such software tools that generate a short numeric or alpha numeric code that expires pretty quickly. This has the advantage that, well, you know, usernames and passwords actually are increasingly guessable. And so even if somebody gets past your username and your password into account, they still have to be able to get past the MFA. There are lots of conversations and debates about the problems with text message based MFA. There are lots of debates about Google authenticator and athe as individual tools go with the concept that any multifactor authentication is better than no multifactor authentication. And just when you have an opportunity to put multifactor authentication on one of your accounts, go for it, go do it.

(11:14):

I am very much enjoying the, the, like, what are your favorite password managers these days? This is good. Good, good re good crowd source resources. All right. 1, 2, 3, 4, 5. So I have five more basics that I'm gonna mention as we go up. So backups using a password manager using MFA, anytime that it is available. The, the next thing to really seriously think about and try to start adopting as a regular ongoing practice is moving from text based SMS based messaging to end it end to end encrypted messaging. So end to end encrypted messaging means if you are messaging with somebody on your telephone, your handhold phone computer, with somebody else on their handhold phone, computer, the message gets encrypted inside the application on your phone. And isn't visible to the operating system. Isn't visible to the cellular network. Isn't visible to all the pipes that go from one cell stand to another cell stand.

(12:24):

Isn't visible to the carrier of the person you're talking to. And it only gets decrypted all the way at the far end in the hands of the person you're trying to communicate with right now, signal is my personal favorite WhatsApp, which is a, I'm just not gonna call 'em Medi yet. Whatsapp, which is a Facebook property is owned by Facebook. Facebook is consistently looking at the metadata and doing some other

things, but any end to end encrypted messaging is better than sending a postcard out over the error. And so adopt end to end encrypted messaging, as you have access to tools. One of the in my world is I have just trained all of my friends and family and colleagues to only talk to me. So yeah, we talk about the stupidest shit on signal. And we do it all the time.

(13:26):

One of the reasons that I do this is what's called cover. So you do not want, if you are somebody who is validly of interest to adversaries, you don't wanna be having like a daily chill hanging out conversation on clear text SMS messages, and then be like, oh, oh, we should swap. We should get on signal. Because the mere fact that you have changed venues, it looks interesting to an adversary. Whereas if you're just using end to end encrypted messaging every day to send dog photos to tell stupid dad jokes, like when you actually have something, a little sensitive to share with somebody you're just doing it the same way that you send the most dumbass things that you would just be posting on the internet anyway. So end to end encrypted messaging is a good thing to do. It is a good thing to do on a regular basis and to start doing like literally for everything you do with your friends, associates, colleagues, family members go for the <inaudible> and encrypted messaging.

(14:35):

Okay. These start to get a little like equivalent. They're not strictly ranked. But one of the other really core things that you wanna do is encrypt your discs. And this is easier and easier every single year. Windows does this Mac does this Mac it's called file vault. I think if you have an iPhone, the iPhone automatically encrypts storage directly on the iPhone. And so usually this is a pretty small step that you take. And the advantage that it gives you is if something happens and somebody gets unauthorized access to something, there's just like one more little step to try and actually get access to the stuff that you have stored. The other reason that it is a really good call to encrypt your discs is if some legally constrained entity gets their hands on your hardware.

(15:35):

It will be much, much harder for them to actually access the material that is on your disc if they don't have here encryption password. So heavily, heavily recommend encrypting your discs. All right. So the, the, the next two are not necessarily for everybody, but I have adopted the hardware keys, one like seamlessly and comfortably. And in fact, I just realized that my hardware key was like literally on my physical keyword this week, cuz I've been running around town a lot. So a hardware key is something like a UBI key. I don't actually know like who the, the most beloved hardware key producers are these days, but instead of hardware key is basically instead of using software multifactor authentication like Google authenticator or athe you have a physical little thing that plugs into a USB port on your computer.

(16:36):

And oh yeah, I am outta date. So I'm not gonna say specific things about like USB versus wireless and Bluetooth and whatnot, cuz I am no longer up to date on that yet, but MFA good choice. U B key, good choice. It is a hardware multifactor authentication mechanism and it's a little harder to great break than software. And I also have to say like from a user experience perspective, super pleasant to just like stick a key in you know, activate it with a little electrical conductive stuff. And then have it provide my multifactor authentication. All right. So the last one that I will mention, cuz it gets talked about a lot is

trying to move over to encrypted email. This was the place that lots of people used to start like 15 years ago, 12 years ago.

(17:32):

It is a really fun space to explore as somebody who likes the cryptography part of crypto and it, and it feels extra, super cool cuz you're like in encrypt shit. The reality is practicing encrypted email messaging is incredibly hard. Email defaults to an open protocol, fire hose mechanism. It is really hard to truly encrypt a message, truly protect the keys truly have it only be decrypted by the person who ought to there are so few me, so few cases in which the right way to communicate is over encrypted email. And so really I put it on here to say like, we can talk about it, but really like you probably don't need to encrypt your email and it can be a fun toy. It can be fun, exploratory space. But it's probably not the thing you really need to invest time and energy in that is there's a fantastic note from ARP, which is never underestimate the importance of feeling really cool.

(18:43):

Yes. That is, that is true being the other thing is don't underestimate the communities you get access to when you start being like I'm on proton mail and only proton mail. Like some people like see you and give you a nod and be like, yes, I recognize my people. And that can be like a trust border over a trust, like tunnel over which you start to talk with people and learn other things. All right. So at the very top of this, like here are the basics. Here are the things that you should think about is like the all seeing eye of nation state actors and non-state actors. If you are the target of a nation state or non-state actor, a really like well resourced and well motivated adversary, these things are still useful to you. But you will need to get introduced to an actual expert and sit down with them and really talk through your specific face and what the actual mitigations are gonna be for you in your specific space. So those are the basics. We're gonna take a breath.

(19:52):

In fact, any advice on finding a specialist, if you do fall, wind up falling into that category?

(19:58):

Well, okay. So that is in fact what we're gonna do next. I, I have advice for like how do you get ready to speak to a specialist? And that's really the threat modeling material I'm gonna walk you through in terms of how to get introduced to one at the I'll I'll paste some links in at the end a number one is anybody, you know, who sort of talks like me and sounds like me and says these ridiculously paranoid things about digital privacy, have a side chat and be like, Hey, who do you know, do you think that you can put me in touch with somebody? Also I have, I have had good experiences sending people to access now, which has a 24 7 digital helpline. Yeah. So that can like help with like a one on one conversation. I suspect that if you sort of dropped a note or when we get to Q and a sort of said like, Hey, who would like to have a side conversation with me about my case and what kind of an expert I need? I dare say a couple of people here will be able to make some introductions. Personally. I do not have deep rich connections in 2022. So I don't have really strong personal recommendations these days.

(21:26):

Okay. So with that, I'm gonna try and go just a little bit faster because oh, I'm gonna use a clay joke. Like I, I never imagined that I would get tired of the sound of my own voice, but I've gotten older and I am very tired of the sound of my own voice. So I'm gonna try and do this in a boat 12 minutes. So there's

some time to like talk and ask questions. So let's get into threat modeling. So threat modeling is literally is, is also known as AKA a piano could fall from the sky, but mostly one doesn't is really easy to listen to stories and to see the media and feel like holy shit, like I'm gonna go to a protest. And then the cops are gonna show up on my door and white supremacists are gonna show up in my door and my life is gonna fall apart. I have worked with a large number of activists over the years. And so few of them have been targeted like this. Some of them have, but it is, it is not a common problem.

(22:32):

<Laugh>

(22:33):

And I really wanna make sure that when you think about going out into the world to try and make change, when you think about your security, think about it from the perspective of creating a sufficient sense of safety for yourself so that you can go out and do the things that you wanna do. There is a pretty clear Antigo, which I have in my notes and apparently I have broken my notes. Hold on one second.

(23:03):

Just sit just so that you can be entertained. Like my notes are literally in VI, like that's how I wrote my notes for today. Okay. So very, very strongly the anti goal. When you sit down and try and think about your personal digital security as a person who might do some things in the world, do not get into the trap of Coplay as some sort of hacker spy and use that as an excuse to withdraw from the world, feel bad about things and not take action. Number one goal, make yourself feel comfortable enough that you feel confident and going out into the world and making changes. So here are the core questions that we talk about. When we talk about threat modeling or setting a safe foundation for yourself, what do you have that you want to protect? Who do you think you need to protect it from what is going to happen?

(23:55):

If it gets compromised and what are the consequences, if it gets compromised, what are the odds like? You may do those three questions and freak yourself out and then think about like frequency and odds and be like, well, yeah, I need to calm the fuck down. <Laugh> and then you get to your action plan. So your action plan will be, now that I know now that I have thought about what the highest risks are and what the most likely things are. What's my action plan for slowly steadily in a stepwise faction, mitigating the most likely and the highest impact risks. So when you think about what do you have that you want to protect? Yeah, didn't, didn't, didn't, didn't proofread my own damn notes. Here are some of the core organizing questions that are useful to think about. So what is the information you have?

(24:50):

What's the data information document slides, videos, photos that no one can access that you have and you want OK. But it's not just about other people getting access to your shit. It is about other people potentially changing it. Think about what would happen if some of the information you had was silently changed and you didn't notice the super important to banks, maybe less important to activists, but it's still a useful lens to put this through. What do you have to protect? One of the things to think about is the integrity of your identity. So making sure that someone else is not pretending to be you, this can be both identity theft on the level of people using your social security number, to open account to somebody, pretending to be you on the internet and damaging your reputation, damaging your ability

to make change in the world because they are pretending to be you and be a different kind of asshole than you actually are.

(25:55):

Other things to think about. And this particularly important these days sorry, this particularly in the news these days is your <inaudible>. So it's not just the address that you live at or the address of the place you go to, but also the travel pattern of where you go, how you go, what the patterns are. We when we think about end to end encrypted messaging, that is O that is most frequently the mitigation for like, what are you communicating? But then you also wanna make sure that you're thinking about who you're communicating with. And back in the day when I did a lot of this, one of the first things I did that I did when somebody was like sent over to me is to be like, okay, like we can't be easily identified as connected because right now I am probably your highest risk.

(26:44):

Like if you connect with me and people notice that they're gonna be like, huh, what's that person doing that I should pay attention to. So you wanna think about who you communicate with, who you are perceived to communicate with and what that network of communicating looks like. You wanna think a little bit about what are you reading? What are you researching? What's the trail that you're leaving behind. And what does it say about the things that you are about to do? Again, I don't wanna make you all paranoid. This is important in some cases and super paranoid in other cases, but it's a good question to like pause and say, you know, I just bought a whole bunch of books. What does that say about me? Should I maybe think about barring reading these in a library rather than having them sent to my home?

(27:33):

And then the last thing to really think about is information about your friends, your family, and associates what the patterns of your children are, whether they go to school on the island or off the island. This can, for some people be very important information to try and preserve and protect because you might be willing to take lots of risks personally, but if somebody threatens somebody that you care about, then, you know, you will just back off and change your behavior immediately. So protecting the information about who your friends, your family and associates are, can be a thing that you decide to do really consciously, not going nearly fast enough. All right, I'm gonna go faster. So the second big bucket is who do you wanna protect it from? Some folks in these categories can be your employer, your future employers, making sure that you have a stable financial footing can be one of the things that makes it possible for you to go out in the world and drive change.

(28:32):

This heading of internet trolls, it's kind of an old phrase for what's really out there these days. Some of these people are people just kinda like bored and getting angry for kicks, but more and more, these are people who are significantly resourced and particularly targeted. And they may seem like strangers and they may actually be people who have vested interest in your actions, thieves, organized crime, consistently a higher and higher threat to everybody who's on the internet because organized crime has figured out how to make a lot of money in really small slices. And so these are some of the adversaries you should think about. And then don't be shy about thinking about the impact of saying something to a family member who either intentionally or unintentionally might be a major source of disclosure and might go pasting your shit all over the internet without having any intention of doing you any harm.

(29:35):

And then of course, we have to keep in mind that some people are genuinely targeted by governments and by large hacker organizations that are highly motivated. And those are, those are real threats sometimes. All right. When you think about what are the consequences, some of the things to think through are harm, and in what way, sometimes you're gonna be thinking about your own risk, but sometimes you'll be thinking about the risks of the people that you're trying to assist the people that you're trying to lift up. And so try to stay aware of what the impact of your actions are on the people you're trying to help and how you might generate consequences for them. When you think about the consequences, try to think real hard also, like it's easy to get like super in your own head about getting safe and getting protected and all of this.

(30:29):

And sometimes like, actually the consequences are really minor and the risk adjusted cost of reacting to a compromise maybe way, way lower than the day to day cost of trying to protect it. And then there is always the consequence space, which is literally like you only live once. Go do it. I'm gonna not tell this anecdote cuz we're recording. But there is a really big piece around somebody sits down and thinks about their threat model starts to think really heavily about their information security footprint and then realizes like actually the things that they're willing to risk are pretty big and they are more interested in making change than they are in protecting themselves from those smaller risks.

(31:21):

All right. So how likely is it that you are going to get compromised? Some of the things to think about are, you know this, this used to come up a lot when people are like super excited about encrypted email, but we're like just publishing their whole lives all over the internet anyway, like step one is how likely are people to just stumble on it because you threw it in the garbage or you put it on Facebook. No equivalence implied. Of course. So some of the stuff that you might do to improve your security, won't be like super badass technical. It'll just be like maybe I shouldn't put a photo of my house on the internet and say getting on a plane and going to Bolivia for three weeks. Like it's, it's it's behaviors like that, that you might wanna think about changing. There is a core unpleasant horrifying fact about our world right now, or at least in the United States right now that there is a baseline of likelihood for all human beings.

(32:22):

And then for anyone who is a woman or non-binary a public figure, a member of an ethnic or a religious minority or in the us people who are black, indigenous and Asian, these people like we have to immediately spin the dial up on their baseline of risk because they are actually targeted at a much higher level at a much higher frequency. And so just by being a member of one of these groups, you're gonna have to sort of like adjust your odds a little higher. Then the other thing to think about when you're thinking about how likely is is a compromise to happen is what kind of resources do your adversaries have? And some of the examples are, you know, somebody who's just got too much fucking a time on their hands and gets something stuck in their CRA and goes like way further than you would expect a normal person to go in researching you or your ship. Nation, state actors, non-state actors are incredibly well resourced. And then this last bullet around natural aggregators is a particularly dated bullet. So I used to think of these as quote unquote, natural aggregators, cuz they were getting collections of data as a side effect of the other things that they were doing. But increasingly under surveillance capitalism, we really see that these organizations are consciously collecting data about every human being on the planet and then reselling that data.

(33:52):

So last one is starting to think about how do you address things and I, I wanna be really honest. I'm not telling you these are specific activities to take. These are some of the things to really think about as you try to build an action plan for yourself. So don't abandon a good process for a perfect process. Lots of people stumble and get stuck because they try and do like the most perfect security and they end up not doing the thing they set out to do in the first place. Cuz they get stuck on the security step. If you got some processes that are reasonably good, just use those, maybe make a plan a month or two from now to like step it up just a little bit. But for plenty of people like they don't need to go to signal if their people are on WhatsApp, if they have a really good pattern of communications on what WhatsApp, maybe that is a fine end to end encrypted message tool to use wherever you can look for a small tweak to a current habit, don't try to change all of your behavior all the time in the physical world.

(34:58):

One of the examples we use is put a shredder directly in front of the recycle bin. So it is easier for somebody to look at the document, be like, oh, that shouldn't persist past today and put it in the shredder instead of putting the shredder down the hall and behind a locked door and making it hard for them to shred their stuff. When you're putting an action plan together for yourself, it is so important to be realistic about the costs. Every step you take to make yourself more secure is gonna generate some friction in your world and it's gonna make it a little harder for you to do something else. So when you're making an action plan, think about how much time it's gonna take out of your life and out of your time out of your day. Think about how much time you're gonna spend, not just getting educated in the first place, but keeping that information up to date and ongoing over time.

(35:52):

There are sometimes the right choice is to just go buy some fucking equipment. <Laugh> go get a second phone, buy a really cheap laptop that you use for your like more sensitive activities. Do some air gaping between your everyday life and your activist life. But be really clear that anything that you do to button your security up is gonna drive a little of your attention. It's gonna make everything just a little bit harder every day. And so choose interventions that are useful and practical for you. Don't try to be perfect. Don't try and do everything at once because very often that learns to a certain kind of InfoSec burnout. And then you just kind of throw your hands up in the air and you give up the last bullet here is about reduction in connectivity. This is a much richer, richer and deeper topic than it was two or three years ago. But one thing that is one of the easiest things you can do is if you're gonna go and try and do something sensitive, just leave all your devices behind, leave your smart, watch behind, just get disconnected for a little bit. And sometimes that is the simplest intervention that makes things a little bit more secure.

(37:07):

That recommendation has changed over time. It is much harder to reduce your connectivity now than ever before. But it can still be like one cheap and easy way to be super secure. Very fast. Last thing that I wanna say is if you go out and start reading up on threat modeling, I, I want you to know that you're gonna E encounter some language. That's pretty like militaristic or like weird. And that terminology is gonna be about assets, adversaries threats, your adversaries capabilities and about mitigation and acceptance. Don't get scared off by that vocabulary. It is literally just the stuff that we have covered here. Hey, one last thing that I wanna say before we switch modes, turn off the recording and have a conversation. And this is what are some things that you can do next? So one is spend a little time with

yourself and think about your threat model, go through some of these questions, do the exercise on paper in private, make yourself an action plan and then, you know, shred all those notes, cuz you've just written down literally how somebody can get in under your skin.

(38:18):

One thing that I genuinely recommend these days is consider setting up 1, 2, 3 sessions with a lawyer or a counselor to help you just talk this shit out, out loud. And it is not because a lawyer or a therapist is gonna be particularly useful. It is because they are legally constrained from retailing, your stories. And so that can be an opportunity for you to really talk through what matters to you and get a lens on. What's gonna set you free to do some things in the real world in a way that you know that nobody else is gonna go gossiping about like, Hey, like what are you really scared of? Alright. I'm gonna paste in now some resources, the very first resources actually just sort of a like reminder of here's something to look out for. I am sharing the New York times how to protect your digital privacy link.

(39:11):

But when I opened it up today, I realized it's undated and there's nothing worse on the planet than an undated security recommendation. It moves really, really fast things change really fast recommendations that I would've made in a fullthroated confident way through years ago. I'm like, I don't know that that's the right choice today. So when you're looking at resources in the world, look for a date, try and sort of suss it a little bit on how old it is. All right. So that's it. That's the end of me ranting. That's the material that I was planning to put in front of you? What terrifying questions? Sorry. I, can you turn off the recording?

(39:53):

Did we, does, do we wanna do like on, on recording questions and then off recording questions, I Don know if anybody has any that they think would be particularly useful to record, but maybe to ask the question first

(40:07):

So one possible on recording question might be, are there resources that were mentioned here, for example, you said pasting in a chat which chat channel is that, that people could go pick up later.

(40:22):

So the chat channel is a thread entitled hamsters workshop on cleaning up your shit to prevent getting docked. And it is in the tabs channel thread, whatever it's called on discord. It's set to archive in one week, but the archived threads are still visible. So once again, the name of that thread is tabs workshop on cleaning up your shit to prevent getting dogs.

(40:50):

Thank you.

(40:53):

I also just put a link to that in the main chat channel.

(41:00):

So are there questions people would like to ask on recording and I'm just gonna ask you to like say yes so that we know to keep recording anybody, wanna ask something on recording?

(41:11):

I think the only one I have is I guess, sort of a statement and a question. I feel like a lot of people in, in tech get really worried. They're gonna be targeted by state actors. And I always tell people like, look, if like Israel targets you, maybe you give up, like you're kind of screwed, but like in your experience, like what's the likelihood of a random person doing like low grade activism being targeted by anyone super serious.

(41:40):

Cool.

(41:42):

We should all be so cool as to gain the eye of terrifying parties. And we are really not that cool. Most of us are so uninteresting to the world. And I, I want you all to take that as reassurance. It is vanishingly rare for somebody to draw the eye of a nation state actor. And at the same time, I will also be honest and mitigate that statement. We have real world examples like Aaron Schwartz, who was making a copy of library resources in a digital closet at MIT as really a protest and as a activism activity. And he drew the ire of the FBI and they pursued him at such an unreasonable rate that he ultimately died of suicide. So it is not a zero chance, but it is a vanishingly small chance. And I wanna advise anyone who's thinking about like making change in the world. I wanna advise you to just start with the fundamentals. And then if you're feeling really nervous, like put a toe in the water and see what feels safe to you and you can take that toe back out of the water.

(43:11):

The highest priority is that you take the power and the privilege that you have access to and you go out and, and make the world better. You don't have to be a frontline activist. You don't have to set yourself on fire, do a hunger strike, throw blood through blood on Donald Rumsfeld's house. Like you individually as a single person are not required to do that stuff, but you are required to do something. The thing that I chose to do was take some of the skills that I have and try and help other people feel safe and help them feel safe through facts and activities and experiences so that they could go out and do the things that they felt driven to do. One of the things that you might do is literally just throw money at problems, go out and donate. That is valuable and it doesn't leave a big trail.

(44:09):

If you wanna donate in cash, you can do that. Do not donate crypto crypto. You that's, that's like a permanent record right there, but like give people money, help other people. There are lots of ways in which you personally can drive a lot of positive change in the world without being on the front page of the New York times. So button up your security to the level that makes you feel safe and do the activities that make you feel safe and support other activists who feel safe, doing bigger things, because it is going to take every single one of us who stop having children get killed in their classrooms.

(44:56):

That was a good mic drop moment, but I'm gonna fuck it up by asking you another question. So you have to keep going. Do you have any recommendations for urging your information from Spokeo people finder type of sites? Because it seems like doing it one at a time is just whackamole.

(45:18):

So right now the, the best resource that I am aware of, and I'm sure there are folks on these calls who have access to other resources, I'm gonna direct you to the freedom of the press foundation page entitled preparing for online harassment. They link out to Penn America's online harassment field manual. I do not know how to pronounce Yale's full name, but the big ass data broker optout list. Freedom press foundation tends to stay pretty up to date and pretty current. And today this page is useful and I have every reason to believe that, you know, going off into the future, this page will also be useful. Ooh. And it has a women, women of color and tech photos on it. That's awesome. I just looked at the image credit, which is the WSC N tech chat photo set. Okay. So that's, that's my recommendation is go look at the freedom of press foundation preparing for online harassment page.

(46:20):

Nice. Thank you.

(46:29):

Okay. So I said that this was gonna go for 50 minutes, which was mostly like we're gonna have 50 minutes of content. I am 100% chill to hang out for another 20 minutes. And that's just to set some boundaries for myself, I guess. What other question? Just noting that we are still recording any other questions that people have for the recording?

(46:59):

Someone put a question in the chat about public wifi that was answered by user VPN in public, but in general, how risky is public wifi and how does like your own cell phones, encryption mitigate that or does it at all?

(47:16):

I am not qualified to answer that question in 2022. Don't do your banking on public wifi. <Laugh> I mean, I, I say that and I laugh like it's self evident and yet I think that that is a good guideline. Don't do it. Don't log into your bank and pay your bills at Starbucks. And also VPNs turn out were, there was a moment in time where information security specialists were heavily advocating for using VPNs. And now we know that some of these VPNs not just pre VPNs, but paid VPNs were aggregating and reselling the usage data from the VPN itself. So this was not this was a recommendation that degraded over time. I, I will be really honest. I think I probably these days trend towards a quote unquote zero trust model where I increasingly believe that any wire I am communicating across is compromised. And as I say that, I realize that's not a helpful answer for this group. Let me go back to my first answer, which is, I apologize, but I'm not qualified to give an answer to that question today.

(48:42):

Are there what, for what it's worth I've, I've played with the tools to spoof wifi networks and like decry stuff running over them. And it's it. This was even a couple years ago. It's extremely easy to do. You can hide the devices to do it anywhere or you could years ago. And I imagine they're only smaller now. So I, I

personally wouldn't trust public wifi for like anything <laugh> I, I would say caveat is like, there's a big difference between public wifi that has no password or a very simple like web password and something like w three, a WP WPA three, which is a little bit more secure, right? There's still ways it can be compromised, but like I would bank over w w P a three God, but I wouldn't do other things.

(49:34):

So this is one of the super fun, like hacker super spy conversations. And I spend some nice part of my life talking about these things the place for anybody who's listening, who's thinking about information security from an activist's perspective. I'm gonna give you the following advice, start with your risk model, start with what you're worried about, and then the things that are important to you to protect don't do, don't do those things on, on the internet. Like try not to do those things on the internet, do those things in an end to end encrypted fashion, do those things in person. But don't, here's my terrible terrifying voice. Do not for one minute, think that a normal human being who doesn't do this as a full-time job can actually day to day accurately assess every network that they might touch, cuz this stuff moves fast. And one of the most dangerous things that you can do to yourself is you can establish a security practice that makes you change your behavior because you think you are safe. So as you choose your action items, as you choose your interventions and your protections, try to BI build big buckets that you can practice consistently.

(51:01):

And do not think that you can do better than a nation state actor on after on a VPN integration. Okay. I think I've just gone way far field and I should shut up

(51:19):

<Laugh>

(51:21):

Back to questions that should be recorded. And I'm gonna try and get myself back in the appropriate lane for this conversation.

(51:29):

Can we get whoever is a plant for like the NSA or the FBI? Can you identify yourself? Can we record that? <Laugh> it's actually it's it's rusty. It's me. It's like who else would on damn. Yeah. Legally, if they're, if you're a cop, you have to tell us that's right. I, your agent I'm all of your FBI agent. I'm just extremely good at it. <Laugh> I think that's probably the end of the recording.