LIVE Weekly Training
Ghost Phone & Tablet
Class #7

Hey everybody. It is Sean Patrick Tario, again, your favorite instructor. We are on class number seven . I'm gonna kick this baby off here and we're gonna learn a whole bunch of stuff today. We're gonna get into the reality of digital privacy, what's possible and what's not. So walking through all the different things we can and can't do.

All the different layers of privacy and concepts of layers of privacy, attaching to different hardware, operating system, application C, communication layers. I'm gonna walk you through all of that today. We're gonna briefly talk about Core boot and firmware. What is Core Boot? I know there are a handful of people talking about this.

I just put a post out about it on our email newsletter. Because I've been getting a lot of questions about it. We're gonna be talking about assessing your personal threat model, which is different for everybody. So we have to understand that what is right for you from a digital privacy perspective is not right for everybody else.

And just because you hear of somebody using some tool doesn't mean that you need to use that tool to be private and secure. Again, this is no different than physical privacy and security. So what's right for someone who lives in a guarded mansion of a house with security gates and security personnel walking around the property doesn't mean that is what you need to also have to be safe.

So we're gonna dig through those different models. We're gonna go through what the practical cost and steps are that you can. Use to enhance your privacy and security. One of the simple things that many of you have already are already doing, and all of this I think is going to lay the foundation so that you can be effective when you're talking to your friends and family about digital privacy and when you're talking to them about why you take it seriously and why they should too.

So with that being said, we're gonna dig through reality versus myth. So perfect privacy doesn't exist, but meaningful privacy is achievable and you just have to understand that, right? That's like saying that, if I'm living in a bunker and I want to be safe, you can totally do that. But. If someone truly wants to find you and exterminate you, they will have the means and motive to do and they can find you and they can terminate you.

Also understanding is, I think many of you already do that privacy is a journey, not a destination. Things are constantly evolving and changing. Yes, it can get frustrating at times especially when companies are bought out or that we discover certain companies that have positioned themselves as being super private and secure.

We realize after the fact that they're really not, that they're just a grift. Very frustrating, especially when you have to migrate email, for example, from one platform to another. I really wanna set expectations. It's not about disappearing completely, it's about controlling what information you share and with whom.

So to disappear online completely is nearly impossible. It's not too dissimilar than trying to disappear on the planet. Again, if someone wants to find you and they have enough means and motive to do they can tap into the satellite network. They can tap into all of the security cameras that are all over the place in cities and start doing facial recognition to try to track down and find someone.

So the objective here is not to disappear completely, but to start controlling your footprint. And we have to start thinking of privacy, like home security. You don't need a fortress. You just need to be secure and not an easy target. So the economics of surveillance is important here. Understanding that what you're trying to do is making yourself expensive to track, making yourself expensive to track.

So all the different things that you're doing and that I'm talking about and that we coach and teach is about making yourself so expensive to track that it's just not worth it for the vast majority of criminals and or agencies to do so with that being said, what we have up here right now is a couple examples of the different layers of security that we have to be mindful of.

And I address this. In a article that I wrote called Can We Really Go Ghost or Is Going Ghost A Myth? And to a degree as I've been saying, it is, it's a myth. You can't really go ghost in the digital domain. What you can do is start to control the data that you are pushing online and you have to start to become aware of the different layers within the IT stack, which those of us who work in the industry refer to it as an IT stack so that you can then address each one.

So obviously we've talked a lot about the operating system level tracking and how Google and Apple and Microsoft and Amazon through their tablets and other tools control the opera operating system. And if they control the operating system, they control the device and the whole business model.

For big tech is really that you're the customer, you're not the customer, you're actually the product. It's because they control the operating system and they control the device. So we won't dig too far down this rabbit hole, the operating system 'cause we've already done so that's why you guys are using Rafino s on the ghost phones to begin with and why some of you have already started the journey or are highly considering the journey of using Linux for your laptops.

'cause that allows you to control the operating system, which is the core brain inside that system. But below the operating system, we have the hardware layers, so firmware and bios and hardware. So there are ways to exploit the hardware and there has, there's been news over the last couple years and there's been all kinds of headlines that talk about how.

China has embedded on motherboards, this little rice looking nodule on the motherboard that was feeding information back to the CCP. When you really dig down that wrap, there was a great headline and it scared a lot of people and it forced a lot of people to really think more critically about the hardware layer, which is good.

But when you really dug into that article and looked at what actually was happening, it was a very select few devices that were owned and controlled by very select nation state actors

where that hardware was picked up on route to the customer and embedded onto that motherboard that then was providing that information back to the ccp.

So that, that is totally possible and it does happen. I'd say every security agency out there has means an ability. To do that, but as we'll get into later, you really have to ask yourself how much time and energy and effort does it take to do that? And are you someone that has to really be concerned about that?

And if you are, what can you do about it? So vol vulnerabilities are harder to exploit and they're also harder to fix because it's not easy to crack open your laptop or your desktop or your phone and see what's really going on under the hood and making sense of what's going on under the hood.

Everything does have potentially a back backdoor access. And we know that Windows, and we know that iOS and Mac Os have backdoor access to our security agencies. We also know that our. Select few agencies have the ability to crack into Intel chips, NVIDIA chips, these other physical hardware layer tools that are embedded in the system.

But the number of people who have the ability to do that and the time and effort it takes to truly identify and go after a device at that layer is extremely high and expensive. Very few people know how to do this as well.

The other key piece here is that the information that is gathered when someone does gain access at that layer is very narrow. So it's a completely different ball game related to me having access to your operating system versus me being able to gain access to your Intel chip. So the information I can gather and glean from what's happening on that device is very limited.

So the use case for someone to want to even do that level of attack or hack into your device is very limited, extremely limited. So when you understand that and you understand the effort it might take for you and cost it might take for you to prevent that type of exploit, you start to think through is it really worth it?

It's like saying, is it really worth it for me to have a security system? That is super expensive and has, turt gunners sitting outside. When I live out in the middle of nowhere, I really don't have very many valuables on my property. And the odds of someone actually trying to bring tanks onto my property to come fight me is near non-existent, right?

So you have to start weighing the cost benefit analysis here. So the other key threat vector is the telecom and carrier level, right? So that's up on the communications side of things. So towers are everywhere and they've built this infrastructure surveillance everywhere, which is why we talk about what an MVNO is, a mobile virtual network operator, a reseller of T-Mobile, at and t and Verizon.

And we've had a class that covered that topic. So I would go back and watch that, those videos. Or that video, so I'm not gonna dig too down into the weeds on that. But there are ways to work around it. So you can work with a reseller who's gonna value your privacy. You can get a new number so that number isn't shared.

You have to be aware of who you're sharing your number with. You can also potentially get a voiceover IP number, which is going to track and not track. It's going to route all of your calls and text messages through the internet, which can be encrypted so that your information is not clearing through the traditional towers and the traditional telecom tower networks and relay networks.

We also have to realize that if we are gonna use a phone, that phone is gonna be constantly pinging nearby towers and creating a location history. So if someone is able to identify that device is tied to this specific person and they're gonna spend the time, energy, and effort to do then being able to track and monitor where you are at any given point of time is totally possible.

So by the simple fact that you're using a smartphone or even a flip phone, you are, you're making yourself available to those towers that are gonna be pinging that device. Those towers may not know what that device is, but if you have your antenna on your device, either your wifi or just your regular carrier network on, it's gonna know that device is at a certain location and it can triangulate and know where you are.

And you might need that for GPS. For, for traveling. So it's a cost benefit analysis here. I need to know where I'm at and if I turn this on, it's gonna make my directions a lot more accurate. So for those who say I, I want to be completely ghost and I don't want to know anyone to know where I am ever, but I still want the convenience of being able to have, traffic updates when I'm trying to get from point A to point B and route guidance and whatnot.

I'm sorry, you can't have both. You have to choose one or the other. So either you get a map or you learn your neighborhood and how to get from pony to point B and you leave your phone at home. Or if you bring your phone, you just have to know that there is a possibility that all that information and that location tracking can be aggregated by someone who may.

Want access to that data. Again, if you don't have an operating system controlled by Google and Apple and Microsoft, you're drastically narrowing the scope of who may even be able to have access to that data. If you're using Graphos, you're drastically eliminating even more of the people that might have access to that data.

But you just have to know that it's a possibility. If I am a person of extreme wealth, if I'm a celebrity, if I'm a journalist who's doing some very targeted information gathering about people who don't want me to be doing that gathering, then I may have to be very careful with how I decide to use those tools.

But if I am average citizen, 99.9% of the population, and I'm doing basic steps. To make sure that my data is my data and I'm not sharing it with anybody and everybody, you can eliminate 99.999% of the threats and the people who may be trying to gather your information and your

data. So with all this being said, you just have to start wrapping your head around the reality that it truly takes over a million dollars and significant bureaucracy to authorize a complex communications hack on an individual.

And it's just not worth it for this bureaucracy and these agencies to do that to every single American mundane American who's just living their life day to day. And you might say I check out a lot of, super, websites about what's happening with human trafficking or what's happening with election integrity or whatever.

I'm probably on a list somewhere. You very well may be on a list somewhere. I most definitely am on those list as well, but I am rather certain based on certain conversations I've had with Intel folks that I am nowhere near at the top of the list as someone that they're gonna start making those investments to truly track every single thing that I'm saying and doing where I'm going and trying to hack through the layers of protection that I've built around my life and around all the things that I do and use on a day-to-day basis.

So am I gonna go spend an additional 10, $15,000 to have additional layers of. Privacy and security when I know I've already eliminated 99.999% of the threats that are out there. The reality is I'm not, and I'm on the front lines now trying to train and educate folks. So when I hear people constantly trying to push, Hey, check out this new thing, buy this new thing, buy this new service.

I view it as hand wavy salesmanship to try to get people to buy the new flashy thing so that they can get transactions and move product and, make money at the end of the day. But is it really necessary? So that's where, I'm my key these days is really, is it really necessary?

Is it absolutely necessary that you take this step, that you do this thing? 'cause in most cases it's really not, and people are overcomplicating this process of trying to get. Safe and trying to get private when they haven't mastered just the basics. And if you want to go and learn, how to become a black belt and how to learn all these special maneuvers and tactics that you can do from a digital domain, go for it.

It's like the, average Joe who wants to go and take a and a special forces ops training class so that they can become a, a master marksman. Totally go for it. If that's what you wanna do, that's what you're into. You want to invest your time and money into that and get into it, go for it.

But is it necessary for everybody to go through the Master Marksman Special Forces Ops class? No, it totally isn't. What is necessary, though, is to have some basic situational awareness, some street smarts, which most of you already have in even getting this far into the class to begin with. So I just wanna lay that foundation here.

With that being said, we're looking at the basic hardware layer. Start starting with the hardware that you can control. Refurbished doesn't just save you money, it can also enhance your privacy. It, I've heard people say you don't wanna buy refurbished some well-known people who have thrown this out there, for what it's worth, these folks that are saying this are coming from a marketing perspective, not necessarily a technological perspective.

And they're saying if you use a refurbished phone, you may have, all of, you may be getting phone calls and text messages from someone who had the IMEI, tied to that device. And, you may have additional, threats of people who are going after that device in the past.

That's ridiculous to me. That's like saying you shouldn't get a brand new phone number because that new phone number you get may also have been tied to somebody. That had some weird stuff going on in their life, the odds of that happening are so slim to none that it's just not even a concern.

So when I hear people trying to spread this fear around not using refurbished devices, whether it's laptops or phones, for me it's a big red flag that someone's just trying to sell me something. So I just wanna put that out there. In buying brand new equipment, brand new hardware has its own issues. It people say, oh, you have potential battery issues with refurbished gear.

Yep, you potentially do, but you also have that with brand new gear. I can't even tell you how many times I've brought, I've bought brand new equipment hardware only to have to return it because something was wrong with it. So it's not just because it's refurbished that there's gonna be an issue with it.

So that's the basic hardware layer stuff. And we've already talked a little bit about that, but let's get into the firmware and bios layer. So the firmware is what makes your device, so the firmware is what wakes up your device before anything else loads. So it's the first thing that triggers, it's the what happens the first few seconds after you press power.

So it's, it starts to think through, okay, what operating system am I gonna load? What hardware is available? What hardware is available to me that's gonna function right now? What hardware do I need? So that's the first few things that pop up. So that's layer two. So layer one being the basic hardware, layer two being your firmware, and the bios in this process, the operating system is the next layer.

So it's the gatekeeper to everything on your device. It speaks up, it speaks down on the device. It's the brain of your device. A an open source operating system means that you have thousands of eyes checking for back doors onto the system. So you have thousands of people, tens of thousands, hundreds of thousands of people using that operating system who know how to look at the code and can see if this operating system, if the code in the operating system is quote unquote, safe or not safe.

With Microsoft, with Mac os, with a lot of these different operating systems. We have no idea with Google, Android, we have no idea what Google Android is really doing, what kind of information it's pulling off of that device because it's closed source. So that's where the operating system is so important.

Because you can start to control your device and make sure that your device is doing only what you tell it to do and nothing else. That next layer up is the application layer and your apps are your window into your digital life and they run on top of the operating system. So that's where that application layer is.

It's above the operating system. Your applications speak to the operating system, and that application may need access to hardware. So it's gonna speak to the operating system, make sure it has access to the hardware, and do a check to make sure that it can or can't. And that's where you can start to control within the application settings.

Do you want this application to have access to your microphone? Do you want it to have access to your camera, to your other applications on the device? That's where the operating system comes in. It's the gatekeeper for. What it's gonna allow or not allow on that device and why we love Graphos so much because that operating system is truly focused on privacy and security at out the gate.

So that's where the applications layer comes in. And then the next layer is obviously your network and your communication. So every connection leaves, breadcrumbs. Every time you connect to something, it's leaving a record, a trail of that. It was connected. Y'all probably don't know this, but if you're walking around, any kind of mall or downtown somewhere, your phone, if you don't turn off your wifi, you don't turn off your Bluetooth.

It's constantly looking out and saying, Hey, I just picked up a new wifi point. That router is also logging and saying, Hey, this device is accessible. Do I want to connect to it or not? So it is a way your phone is constantly trying to connect. It's constantly talking to all the different things around you.

And if you don't turn that those things off when you're out in public or throw your phone in a Faraday bag, then it's gonna start leaving breadcrumbs as to where you were. So if I can track the IMEI number on your phone or your device, your laptop and the WiFi's on, I can start to track where you were, where you went, what you were doing.

So that's where you have to just be aware of this stuff. This is part of the lifestyle changes that people have to start to make so that they realize that this device is truly a mobile tracking device. You maybe don't need to bring this with you everywhere all the time. Maybe you could leave it home, maybe you could leave it in your car, maybe you can throw it in a Faraday bag.

Maybe you can get one of those slips that's like a Faraday pouch that you can throw your phone. Into and throw it in your pocket or your your purse.

So comms are important. Encrypted comms are important. Learning how to use encrypted communications. Learning that just because you are using an encrypted communication tool like Signal and you're using a device that's private in an operating system, that's that's also open source and private and secure doesn't mean that the person on the other end who's also using Signal is also gonna be private.

They may be running Mac Os, they may be running Windows. And as a result of that, they are essentially providing the whole phone call record to their device to be recorded. So it's the same thing with email. You might be using an encrypted email service, but if you email a Gmail account, you now just have to know Google's gonna have a recording of this conversation and they're gonna know what email it came from.

They're gonna know a lot of information about who sent it and the content of that email. So when you start looking at layers of privacy as a whole, you can start to put together a systematic approach and say, what are the things I can control? What are the things that are easy for me to control and affordable for me to control?

And what are the things that when I can get around to doing it, I will jump at and I will start to attack when I can, when I have the time, and when I understand the other basics so that I can start building on this layers of knowledge that I'm gaining. The chain the whole concept of a chain is only as strong as its weakest link is very important.

Security at one layer can be undermined by weakness at another layer. So this is where, things start to get overwhelming for some people and they're like, oh, this is too complicated. And I say, it is complicated. And you might just wanna simplify your life and get rid of a lot of the tools.

Get rid of a lot of the applications that you think you need on your phone that you really don't need on your phone. There's no reason to have a banking application on your phone. There's no reason to have a lot of these different app, social media apps on your phone. You can keep those on your laptop that are safely in your home, behind a firewall in your home.

There's a lot of things that you can do from your laptop and should be doing from your laptop that you don't need to do from your phone, that you carry around with you all the time everywhere you go. So there's a lot of different. Hardware and firmware realities that we need to be aware of and just understand.

The whole pixel phone ecosystem is important for people to understand. I think most of you have already gotten through this and passed this, but I do get this question often as to, but you're using a Google device. I say, yep, we are using a Google device. But we strip all the Google software off that device.

And people say how do you know Google hasn't embedded any kind of firmware or hardware that's gonna speak back to the mothership? It's because we've tested and we've been testing and we have a community of people who are constantly testing the devices to make sure that there's no hidden signal or hidden message or hidden content that's being sent backdoor to the likes of Google or anyone else.

It's not too complicated to run those tests, and those tests are constantly being run on the new pixel devices. Is, so that's how we know and the Pixel device was specifically designed for the Android framework, open source, Android Framework. That's why, Google was involved in the development of the device because they wanted Pixel to be optimized for open source Android so that the core of their system, which is based on open source Android, could be optimized.

That's why Graphos uses Pixel. 'cause there's also very significant security and privacy features within the Pixel that make it so that you can sandbox different application environments so that we can actually, it's interesting enough, Google's involvement with the development of the Pixel device to be optimized for Android has allowed it so that we can actually remove Google from the device.

Which is an interesting thing, but it's a reality. And I, I've gone into the whole argument around refurbished versus new hardware. I spoke briefly about it just moments ago but I strongly and vehemently am anti, new thing. Creating more demand for exploitive mining practices around the world.

For all the new minerals that have to be mined in order to go into these new devices. There's over 15 billion phones for 8 billion people. Most people are getting new devices every two, three years, which means you have all these billions of phones that are available on the marketplace that other people can use.

And that's what we've been able to tap into doing what we do to provide the service that we provide. Big proponent of refurbished versus brand new hardware. The other important concept here is that there's no such thing as Google hardware or Apple hardware. They're just components that Google and Apple have specified.

So Google goes to the manufacturer and says, we would like a device that has the capability to do X, Y, and Z. And then the manufacturer is responsible for assembling that those components onto the device. HP and Dell, for example, are literally manufactured out of the same facility. It's a massive facility.

They're manufactured out the same facility, and they just slap a different logo on the hardware. And obviously there's some design differences between the two, but they're, they all come out of the same facility. So it's mostly commodity parts with minor customizations that are going on within these pieces of hardware.

That even goes with the Cleo line, which is what System 76 and what laptops with Linux and all these other companies are offering. They are commodity parts, commodity hardware assembled together. So that now leads into the whole concept. We've heard about Core Boot, we've got different people talking about how important Core Boot is and Pure Boot is and what is it?

So I wrote it, I wrote a post on this, God, six months ago, probably more than that. And it's come back into the picture recently and I just want people to know that Core Boot, first you have to wrap here. What is it? It is a open source firmware layer. So it's an open source firmware layer and that means.

That you have to program that firmware to be able to speak to hardware and speak to an operating system. So when people ask do the laptops that you offer run Core Boot, the answer is for us with the systems that we offer, which are Lenovo and hp, and Dell is no, because Core Boot doesn't run on any hp, Dell, or Lenovo devices currently, there's only a very small select few devices that even run Core Boot right now because it's extremely complicated and difficult to write code, firmware code to make it so that any operating system can be compatible with any piece of hardware.

And to put this into perspective, I'm willing to bet that most of you have wasted, God knows how many hours of your life trying to get your printer. Which is a piece of hardware to connect to your laptop or even your phone, and that is because the printer, just think of it as an external piece of hardware that needs to speak to the operating system of the device.

So there has to be firmware that allows for that connection to happen. To speak between the operating system and the piece of hardware. It's difficult. That's why a lot of times people have to download mountains of software to just get a printer to work with their laptop. I can tell you I've literally wasted weeks of my life at this point trying to get printers to work with various different devices, even when it was supposed to be super simple and easy to do.

It's not easy. So there's very few laptops. That are actually capable of running Core Boot, this open source firmware layer core boot, and there's very few hardware components that are also capable and interoperable with that open source firmware layer as well. So the reason why we aren't actively selling Core Boot is A, the ability for someone to exploit any kind of vulnerability on the firmware layer is so slim to none right now that it's negligible to even worry about, especially for the vast majority of consumers.

B, because it's super expensive to buy a device right now that is even running Core Boot from Pure Boot. It's two to three times as expensive as other options on the market. And the third reason is you have only very few options as to what hardware, what laptops and desktops you can even use. With that firmware, open source firmware, core boot running.

So it's just important to understand that. And the people who say you have to have Core Boot if you want to have a safe and secure laptop, I think are over-inflating the need for this. And it's primarily, I would say, driven by the desire for people to sell more expensive laptops. The first thing that we need to cover here, folks, is getting the operating system that you're using changed.

The second thing is getting the applications that you use changed. And the third thing is making sure that you're using the communication tools in a safe and effective way that covers the vast majority of the risk that general consumer has in the marketplace. So hopefully that makes sense. And when people start asking you about Core Boot, they start asking about.

These questions, you can have an understanding of what's actually happening here.

So where do we want to spend money on the privacy spectrum or where do you sit in the privacy spectrum? This is, I think, a great graphic for you to start wrapping your head around this. It's privacy exists on a spectrum. Where are you at with it? Are you completely exposed? Are you, do you have maximum privacy in, where do you fit somewhere in, in that scene?

I can tell you that the reasonably private vector here should probably be far further to the right because if you are running Graphene os with basic privacy apps, you are mostly covered. You're mostly get you, you can take the time to learn how to use a VPN. How to use encrypted comms, how and what core boot is.

And if you want to spend the money to get a device that's gonna cost you around a thousand bucks, at least for a basic system go forth. If that's really what you want to do, I would say you don't need to do that. 'cause the people are gonna exploit the firmware layer again, are slim to none for most people, the vast majority of PE people.

So why spend a thousand dollars to solve a $10 problem at the end of the day is the way I look at it. And we need to address the threats that we're actually facing before we start addressing the theoretical ones that we might maybe facing. If we become a super spook starting with the operating system, starting with your applications, starting with your network security and the communication applications, that's where we're gonna solve for the vast majority.

Of the problems.

So privacy cost versus benefits. This is, I think, so key for most people is a conversation that is not being had. So we have on the x axis here, effort and cost low to high, and we have the privacy benefit low to high. Changing your browser is big. That helps solve a lot of the tracking that's going on online.

If you go to amazon.com for example, and you're using a traditional, Microsoft browser or Google browser, a Google and Microsoft are gonna be tracking everything you're doing and feeding that data into their system. But if you go to Amazon on top of that, Amazon is now gonna start embedding cookies onto your system or Facebook.

Is gonna start. They're super sophisticated in how they do it, but they embed cookies on your browser so that they can start tracking everywhere you're going online. So using the right browser helps prevent that. But as we were talking about the operating system is the key component here because I can be using Brave Browser on a Microsoft Windows device or a Mac OS device, and Google and Apple are still gonna gain access to everything I'm doing 'cause they can see everything that I see and hear everything that I hear.

Changing the operating system is that 80 20 rule. So if you can change your operating system and change your browser, you've solved for 80% of the problem that you're trying to solve for. Using encrypt encrypted communications devices solves for an additional, let's just say 10% of the problem using a smart carrier.

We're using a voiceover ip phone number that solves for another, 9.999% of the problem that we're trying to solve for that last layer of the firmware and Core boot, I say solves for 0.0001% of your privacy. And it's gonna cost you a premium to solve for that last remaining bit, right? So if you want to do it, you totally can, but what are we really trying to solve for here?

And is it worth it at the end of the day? So the reason why you see communications encrypted and Security Network on the higher end of the scale here, it's not so much because the cost to do so is high. It's because the effort to do so is high. Learning how to use these tools, install these tools, learning how to migrate.

These applications from one device to another device. Learning how to set up and configure your home network, your home firewall, that takes time, energy, and effort. Very rarely can you just buy something out of the box that's just going to work. You have to do some configuration, you have to do some setup.

You have to understand how that thing works in order for it to actually serve the purpose that you intend for it to purpose or that you intend for it to accomplish. So it's important to look at this and understand what am I gonna do that's low effort, low cost to get me the most benefit? And that's changing your browser, changing your operating system, using some encrypted communications.

And then you can start digging through your FI local firewall. Your local security. And then the last thing, if you really want to go down and spend the money to do to protect yourself from a threat that's like really non existent, you can then go through that core boot firmware upgrade as well.

Hopefully that makes sense for folks.

So I just want to rehash and further dig into and lay out some of the most practical applications for security. And one of those is gonna be essential app permissions management. So just because an app asks for permission doesn't mean that you need to grant it. That is the case with all the different apps that you download, regardless of where you download it from, regardless of whether that app says that it's safe or not safe, or that it has a low risk or a high risk.

When you download that app, a new app onto your device, you should be going into the settings and you should be looking at permissions and seeing what permissions this app does or does not have access to, and start learning what those permissions mean so that you can then be faster at doing this in the future if you use an app on a regular basis, just because it's preloaded on the phone.

Just because we as a company, mark three seven preloads an app on the device doesn't mean that you should just. Carte blanche think that it's gonna be totally fine and totally okay. As a best practice, you should be going into the app. If you're gonna use it on a regular basis, see what permissions it has, make sure that it's only got those permissions and access while the app is running.

And if you're not using the app, uninstall it, get rid of it. You don't need it. So just uninstall it. Of the 40 some odd apps that are, that come on the device, I would say most people can literally purge about two thirds of them, if not more, that they just won't use or know that they're not gonna use. If you're not using the app, it doesn't need to sit there cluttering up your phone, get rid of it and just check for it.

So using another practical application would be the alternative app stores and safe installation practices like I've been saying. Asteroid and Aurora are great. They're vetted privacy respecting applications that you can use to download and view apps. You're constantly gonna want to be looking for updates.

You're gonna be looking for a developer reputation before installing. I walked through that in one of the last classes as well as how to and what to look for as it relates to that when the last time they did an update to the app. Is also something you can look for. So another practical application would be communication tools.

Using signal session element end-to-end encryption is the baseline. It's not the complete solution, but we're looking for an end-to-end encryption tool communication tool. Your communication is really only gonna be as secure as both ends of the conversation, as I've been saying repeatedly, over and over again, just because you're using Signal doesn't mean that it's gonna be safe and secure because the person who's using it on the other end may be using a device that is recording your conversation.

So you just have to understand that and wrap your head around it. The weakest link principle is absolutely paramount. You just have to start wrapping your head around it. You can't say, you can't say and claim that you're, you're doing everything you can from a security perspective, if you're constantly messaging and texting and calling people from a device that you want to be super private and secure, who are using not private and insecure devices.

So on my end, because of the nature of the work that I do, I've taken an additional step and that I have multiple devices. I have one device that I only use when I know I'm communicating with people that also have private and secure devices and take their privacy seriously. And then I have another device that I use for my public domain for a lot of the incoming stuff that I do with customers, because most of my customers, before they.

Become customers who were calling me, asking me questions that are using devices that are not private and secure. So I have numbers and I have devices that I use in the public domain, and then I have numbers and devices that I use in the private domain.

So the more you convert your friends and family to secure platforms is going to multiply your own security. So just think of it that way. That's one of the things you just have to keep in the back of your mind as you're talking to your family, that the more of your family and friends you get to start using these devices, the more private and secure they're gonna be, and you're gonna be by proxy.

So the next major topic I want to cover here is the realistic assessment framework. Looking at our threat model matrix, where do we sit in this domain? This is what I've been talking about over and over again. Identifying your actual privacy needs. Who are you trying to protect your data from? Big tech, government criminals, and understanding that different threats require different countermeasures.

So most of us just need basic privacy hygiene. That's the vast majority of the public needs basic privacy hygiene, because we're operating with zero privacy hygiene. We've outsourced this privacy to companies like Google and Apple and Microsoft who have told us, Hey, we care about your privacy. Apple is privacy, and yet we learn that apple's really not privacy, that Google's really not privacy.

That these, their version of privacy is they get access to all of your information and data. They can share it, but we may prevent other people from getting access to your information. So are you a high value target? If you are, then you have different considerations and you might need to invest more time and money into protecting your stuff.

Versus being an everyday, just basic situational awareness from a privacy domain as we've covered, right? Your operating system, your browser, your communication tools, that covers

the vast majority of it. If I'm Tucker Carlson, I'm gonna have a whole different attitude towards my digital privacy and security.

I'm gonna have to spend probably tens, if not hundreds of thousands of dollars to make darn sure that not just myself, but my whole network is locked down. And it baffles me that so many people don't do that. And yet they wonder how easy it is for people to hack into their environments. Most of us are simply not worth a million dollar hacking operation, which is what it costs.

To go after someone at that firmware layer, level and layer, and to go after people who are using that basic baseline level of, securing private operating systems, securing pri private communications. If I'm doing all of that, I make it extremely difficult for a hacker to come after me and try to hack into everything that I'm doing.

So we need to balance convenience, cost, and security. Perfect. Security with zero convenience is just not sustainable. It's just not possible. So you're. Perfect security. You're going, if I'm Trump right, or if I'm, I just heard VP Vance being interviewed by Tucker Carlson, and he was asked, what's this new life like?

You as a vp? And he was talking I can't really go out in public and do a lot of the stuff that I used to do anymore. People know who I am, people know where I'm going. And so we have to actually tell the secret service where we're going and what we're gonna do, and we have to be a little bit more considerate about what we're gonna do and where we're gonna go as a result of that.

It's the same thing with your digital domain. If you are of that level of importance and you have that level of visibility, the steps you have to take are different than average person. So finding that, that balance point where your security doesn't become a burden, both financially and from a convenience perspective is absolutely key.

And going back to that 80 20 rule that we just looked at, 20% of the effort will get you 80% of the benefits. I would even say 20% of the effort gets you 99% of the privacy benefits. So you want to focus on the high impact, low effort changes first. That's part of the journey. That's part of why I've been having you guys map out what's going on in your world and what's important, so you can slowly and meticulously start going through and doing all this.

So the average privacy conscious consumer making simple changes like using Graphene os, using signal and a privacy focused browser like Brave is going to get you where you need to be. Making yourself a harder target than 99% of the rest of the population that hasn't started making these changes yet is absolutely key.

If you're a small business owner or an entrepreneur, if you definitely wanna start protecting your data, your property. The communications that you're using, separating your business in personal and digital lives, that's absolutely paramount. Like I was saying, having separate devices is probably something you wanna do.

I was just at a conference down in Florida talking to a handful of attorneys and one of the major attorneys for one of the major firms in the data center industry. As we were talking about privacy and security, and I was walking him through everything that I do. It started to dawn on him.

He's holy smokes. I have all of my personal stuff and all of my business stuff on the same Apple device. That's probably not okay. And I was like, that's most definitely not okay, man. Like a hundred percent. That's not okay. And his coworker was like he has two separate devices, one for his personal, one for his business.

He does not let them. Crossover. He's very strict about it. And he started actually selling his business partner on why he needs to have two separate devices. So that's very important. We need to keep those things separate. If you're a activist and a journalist you need to use more sophisticated tools.

That's just the reality of it. You the stakes are gonna be a little bit higher for you because you have more people eyes on you. You're putting yourself in a position where you're, understand that you're gonna be at risk. And so you have to take a few more precautions. It's, someone who's constantly traveling on airplanes, someone who's constantly going into business meetings all over the country, all over the world, that person is in a different paradigm than grandma, grandpa, who really only goes to the store every now and again.

And likes to FaceTime with their grandkids every now and again, like different paradigms, right? So dealing with high risk individuals, super wealthy people. If you have a lot of crypto, this is where, when we're looking at network service providers and we talk about, when is it is it good to spend a hundred dollars a month and use a service like Ani, which you all have probably heard of Ani offers a $3 million liability policy.

If someone steals your sim card, steal, steals your identity, that's worth it. If I use two factor authentication and I lose a lot, if someone steals my phone number, then I'm probably gonna want to pay the premium for that level of service. But again, if I'm grandma, grandpa, I'm not, I don't have millions of dollars in crypto.

I don't have millions of dollars in a bank account that I'm trying to protect. Probably not worth the a hundred dollars a month. I can probably get by using someone like Pure Talk or someone like Patriot Mobile who is not going to proactively give all of my information to the carrier that they're reselling so that they know exactly who I am, where I live, you know everything about me.

But I also have to personally take responsibility and make some lifestyle changes and saying, I'm not going to give my phone number out to everybody who asked for it. You don't have to give your information out just because someone asked for it. If phone number's listed on the signup form for something and you don't need to give your phone number, don't give it.

And if you do have to give your phone number out to a lot of people, but you're a more high risk person, maybe you get two phone numbers, maybe you get three phone numbers so that you can compartmentalize and have a phone number that's in the public domain and a phone number that you keep in the private domain.

These are the types of lifestyle changes we have to think through when we're going through the process.

So some more real world privacy limit, limits and limitations that we need to be thinking about. What tracking is genuinely unavoidable. So your digital existence is gonna leave a trace, and our goal is to minimize, not necessarily eliminate them. If you want to eliminate it entirely, then eliminate all your devices.

It's, you just have to think of it that way. You have to, if you want to have zero footprint from a digital perspective, you may as well just have zero electronics around your house, in your house that you use on a regular basis. You just have to realize that my goal is to minimize the threats, not necessarily eliminate all of them, because it's nearly impossible to eliminate all of them if you're gonna exist in the digital domain.

The surveillance infrastructure, the surveillance economy, it's literally built into the, modern society. Had a customer just the other day said, Hey I want to go to a Bob Dylan concert but I need to buy my ticket through Ticketmaster. And I have two options. I can either go to the venue an hour and a half in advance, prove who I am and get my ticket, or I can download the app onto my device and download the ticket and then uninstall the app.

What should I do? How can I safely download the Ticketmaster application and get what I need without it getting access to all my stuff? I walked him through what private spaces was on the device. I walked him through setting up a new user account. But at the end of the day, if he wants the convenience of just being able to download the ticket and show his phone, then.

That's, he's gonna have to accept that he has to download that app onto his device. Personally, I think it's ludicrous. I think it's discriminatory that these companies are forcing people to use these types of devices in order to gain access. But it's obvious as to why they want to do it. They want you to download that app because once you download the app, they get access and they get all your information and they can sell your data.

So it's just there's some tracking that is gonna be unavoidable if you choose to use certain things in society today. You just have to understand that you can choose an opt out if you want to, but you may limit the convenience. You may limit what you can or can't do. You may have to show up to an event an hour and a half early just to get in.

You may have to do those things. So the other real world I. Yeah. Perspective is that the community hide mind insecurity is very real. It's a great thing from an open source perspective. But it's also a bad thing that has evolved over time because we have a community that has simply trusted that all of these different companies are safe and we've outsourced our trust and our safety to companies that do not have our best interest of mind.

So we're constantly fighting a mentality of people who are like, eh, so what? And we're gonna get into this towards the end, but one of those conversations that you have, what you can have with your friends and family is that, if I were to walk behind you all day, every day and literally be writing down everything that you're saying, everything that you're doing, and tracking everything that you're saying and doing.

You would probably get a restraining order from me and call the police and make sure that I can't do all those things when I'm walking behind you and following you everywhere you go. And yet we have allowed for Google and Apple and Microsoft and these other companies to have that level of access and deeper access.

Everything that we buy, like everything that we do, they have all of this access and we've just given it to them. So that's part of the conversation, do you value your privacy and your security? It's a simple question. People, most people will say, yeah, I value it. Then you can throw that. If I were to follow behind you all day every day and blah, blah, blah, how would you feel about that?

People are like, that's, I wouldn't feel cool about that. He was like why are you cool with Apple and Google and Microsoft doing that to you all day every day? As we've mentioned, the open source model and framework is great because it gives thousands of eyes watching for problems with.

With code. Just because something is open source doesn't mean that it's perfect, doesn't mean that it's gonna be safe. It's where the number of people using the tool is important. The number of updates that they're pushing out, the number of people on the team that's responsible for managing the software is important.

But we should no longer just be trusting companies because they say we should trust 'em. The other thing that we can be doing is planning for privacy breaches and realizing that we're probably not gonna be able to prevent all of them. It's no different than having a backup plan for your data. The reality is that your phone may drop and break, and if all of your data's on that phone and you can't access that data, your SOL.

So if you're not regularly doing a backup of the things that you think are absolutely essential and important that are on that device, whether it's your laptop or your phone or whatever, then that's a problem. You need to create countermeasures so that if and when disaster strikes, you have a backup.

And we have to realize that nearly every major government system and major corporation system is likely gonna be hacked. So if your data is sitting despite, HIPAA rules and despite financial companies having so many layers of security, they are all still hacked and hackable. And because they're worth so much, all that data is worth so much money.

People are gonna invest the tens of millions, if not hundreds of millions of dollars into trying to subvert and gain control and access of those companies. And thus the data. That's within those companies. So that's just a reality. So what can we do about it? We can prevent how much data we give these companies.

We can maybe, if it's not essential for sign up and registration stuff, give false information, we can not necessarily have to put your name or your phone number or your email address or create pseudonym emails or pseudonym addresses that you can put down instead of your actual information. So there's lots of different things that, that we can do.

We just have to become more situationally aware.

So this last section that I'm gonna be focused on here is communicating digital privacy to others. So the, I have nothing to hide. Comment drives me insane. I'm sure you guys probably hear it all the time, but it's not about having something to hide. It's about having something to protect. Would you let someone read all your email, even if you're not a cri criminal, would you let someone stand behind you and read all your text messages?

Probably not, definitely not right. It's no different than saying that your First Amendment doesn't matter because you have nothing to, offensive to say first Amendment most your freedom of speech. Most definitely matter matters. The Second Amendment doesn't matter because, I'm not really planning on shooting anybody today sure.

Take my guns. No, I'm not planning on shooting anybody, but you should not dictate whether I should or should not, or cannot purchase and own a firearm. The people who say it's too technical, it's too complicated. I'm sure some of you fell in that camp when you first started thinking about going through this process, or you even started going through the process, but you don't need to understand how a car works to drive one.

It's important if you want to, help yourself if disaster strikes to know how your car works so that you can change a tire, you can change the oil, you can open the hood and see what might be going on. You know when to actually take your car in to, to have an oil change, to check your tires.

Air pressure every now and again. You know how to read the controls and the monitors on the screen. So if it might be overheating, like all that stuff is important to know and it makes you a better user of the tool. As you start using these things, you can start to learn how to become better, more efficient, more effective users of these tools, and then help the people around you with it as well.

And starting with simple changes makes a huge difference. It's a step by step journey. That's why we have the journey map up here right now. You don't have to do it all at once. It's a journey. It's a process. Start with what's easy and simple and then slowly build from there. Don't move on to something complex until you've mastered the easy stuff first.

So those who say it's too technical, it's too complicated, I don't have the time. Literally have customers who within five minutes are up and running, and I have some customers who within five weeks are still working at it. Everybody's different. Everybody goes at different stages. Different people have different technical skill sets and backgrounds.

So we just wanna reach people where they're at and help guide them. Along the way, but that's why we have lots of different tools, videos, guides to help.

The other reality here is that privacy gets more convenient as you adapt to new habits. So the better habits you have, just like with your diet and exercise, the easier it's gonna get. You may become addicted to these new privacy habits, just as we've been addicted to the lack of privacy habits.

Just like people get addicted to working out. If I go more than a day or two without hitting the gym, my body starts telling me, Hey bro, get back to the gym. My body wants those endorphins being released. I need that because of, the anxiety and the stress in my life.

If I don't have an exit for that, I know it's gonna start manifesting itself in other ways. So I've become addicted now to living a healthier life because I know if I don't, the bad things that are gonna happen are gonna be far worse. So we can start to build these habits into our life that become things that we want to do and want to have.

And the inconvenience of identity theft is so much greater, right? So those who say it's too inconvenient how inconvenient is it when you get your identity stolen? How inconvenient is it knowing that all of your data is being aggregated and sold in the open market to the highest bidder? That's, for me that's a big thing.

That's an inconvenience that people don't even think about, or most people aren't even aware of that's happening.

So the other common resistance point that I get is a black pill, which is everyone's tracking me anyway. So you know what's the point? And my response is, partial privacy is really far better than no privacy at all. So just because there's so much poison in the food that we eat, that we buy at the grocery store, we get from fast food restaurants doesn't mean I'm not gonna try to eat healthy.

It doesn't mean I'm not gonna try to grow some of my own food. It doesn't mean that I'm not going to look for companies that have as a best practice growing things that are organic free from pesticides and not throwing additional added chemicals and preservatives into. They're food. So I'm going to take the steps that I need to do in order to live a healthier life, which is the same thing that we can do with our privacy.

They're simple, easy things that we can do that are not inconvenient to start to reclaim our privacy, reclaim our data. And it's not about controlling it, it's, I'm sorry. It's all about controlling who has our data and not necessarily eliminating all tracking all together. Again, if we are gonna be living in the digital domain, we just have to know and realize that there, there may be some tracking going on.

It may be extremely difficult for people to gain access to that tracking, and that's what we want it to be. We just wanna make it extremely difficult and hard and costly for someone who says, Hey, I want to gain access to this person's information. How can I do and they might hit some roadblocks and be like, I just, this is I'm gonna need to get approvals.

And spend, get some additional resources on this case to do is it really worth it versus just going to the next person who's openly sharing on Facebook and Instagram and TikTok and is using Google or Apple and is using all these other systems that are just freely and willingly giving them all the information that they may want or need about them.

So when we're talking to our friends and family, we obviously wanna start with relatable concerns. Connecting privacy to things that people care about already. You wanna make it

personal. So their bank account, their medical records, their children's photos that are being posted online. Obviously using analogies that connect with people.

Digital privacy is like having curtains on your windows of your house. Your data is like your wallets and you don't want to hand it out to strangers. You've heard me give multiple analogies, as it relates to firearms and how. Learning how to use a firearm is absolutely essential. Just by owning one doesn't make you safe.

You're, in fact, you're more of a threat to yourself and the people around you if you don't know how to use it. It's the same thing with these tools. If we don't know what's happening with them and how to use them, then we're more of a threat to ourself and the people around us. The other key here is we want to do progressive introductions of thoughts and ideas versus overwhelming them with information.

I think for those of us who are on the front lines, fighting back against Covid, I that's we've learned that, you can't overwhelm people with data and overwhelm people with stories. You have to give them, bite-sized pieces at a time, see if they're gonna take, even, take that nibble.

And if they are, then we can build on that versus just flooding people with a dozen different links and interviews and podcasts and people are like, they just write you off instantly. So we just have to do a slow drip approach. The journey of a thousand miles begins with a single step, right? So we have to just take a step.

We have to introduce the idea, try to make it land with something relatable, and hopefully get people to slowly start to take a seriously and start to make the shift. And there's different solutions for different technical comfort levels, right? People don't have to just instantly jump in over their head and start using a completely different device.

This is why I am a big advocate of those mic locks, which I think I've talked to you all about which you can plug into your device and you can essentially mute your device. That's why it's called a mic lock. So it, it convinces the device that it is receiving a audio signal, but it sends a null signal.

Into the device. So when you plug it into your iPhone or you plug it into your Google Android phone, it's essentially going to mute the mic on the phone. So your phone is not listening to you all the time. Some people, that's simple, it's like a $20, $15 fix for that, right? Doesn't solve the operating system problem, but it solves that problem.

And if that's the foot in the door that you can get people to, to bite on and get them interested in starting to ask more questions, then that's a great foot in the door. As I've done events all over the country, people are very apt to make that, $20, $40 investment in their digital privacy to solve for that problem.

And then that really gets them asking more questions, and then a month later, six months later, they're like, Hey, tell me more about those devices that you had as well. So we just need to start where people are willing to engage, both from a financial perspective, but also from a technical knowledge perspective.

Your own privacy and security is important to nearly everybody, whether you're a Democrat or Republican, whether you are a Muslim or a Christian, whether you're an atheist, it doesn't matter whether you're a libertarian, like for most libertarians, you definitely care about your privacy and security.

So this privacy and security talk is really relevant to everybody. There's very I really, I could only think of one person that I've met. Who, when I asked them, how do you feel about the fact that Apple and Google and Microsoft are literally tracking and monitoring everything you say and do?

Wasn't like, yeah, I'm not okay with it. I did talk to one person who was like, yeah, I don't think it's a problem. I'm actually a big advocate of it because it makes my life, so much simpler and easier. And I've talked to, at this point, tens of thousands of people over the last couple years about this.

So I've seen it crosses all denominational lines. It is agnostic from a topic issue to bring up with people.

So what I'm really trying to do here and what I think we're all trying to do here is just build a community of people who are working on this stuff together. I wanna share what's working. And learn from each other's experiences. That's what that FAQ is on the website and what the troubleshooting guide is, and all the content that I have.

If someone asks me a question that's a new question that I haven't answered before, when I answer it, I try to take that question and answer and I try to push it into the repository of information that we have. We should all be doing that and sharing that information. It makes us all better as we go through this process.

I try to approach everything without judgment when I'm talking to people. Everyone has to start somewhere in this process. Even if it means telling people straight up that they need to go backwards, that a flip phone is a better option for them. And if they need to have a GPS tracking for their car when they're traveling, get a Garmin device and just put that in your car.

Making progress in your digital privacy world matters more than perfection. So we want progress versus perfection. So let's just slowly move forward, making progress and acknowledge, acknowledge wins. So many of you have made a lot of progress over the last couple weeks and months. Amen.

Hallelujah. Great work. You can always take steps moving forward. So even the black belts in, any martial art is still gonna be learning, constantly learning. I am still learning new stuff every day, and that's, for me that's awesome. It's frustrating at times, for sure. But there's always new things to learn and it's constantly evolving and changing.

Just like physical security. People are always finding creative new ways to use new things and new tools that are available to try to find. Access to your money at the end of the day. So we have to respond in kind and realize that we have to learn through this process. It's a marathon, it's not a sprint.

We're building privacy habits that are gonna last a lifetime and hopefully that we can share with our significant others and our kids and our family and friends. That's what's important here. As just a quick recap, we're talking about privacy existing on a spectrum. You have to figure out where you exist in that spec spectrum so that you know what effort and money you should be putting on the table to get you where you need to go.

You want to focus on what's gonna create the highest impact first. And we want to really build a privacy conscious community of people who can help one another. We also want realistic privacy. Roadmaps based on where we sit on that matrix on that threat model matrix. So we're not spending tens of thousands of dollars to become, the special forces ninja of privacy and security if it's totally unnecessary, and we don't have to have the expectation that we need to achieve that.

If our goal is just to have basic situational awareness, basic privacy, and security, you're not putting yourself at risk all the time. You don't need to go down that rabbit hole. You can if you want to, but you don't need to. So setting achievable milestones is important, which is why I had you guys working on creating those maps, those roadmaps early on in the class.

So we're here to support you. MARK37 is here to support you. If you have additional questions, you know where to go to get them answered. Support@MARK37.com. You can do our live chat, you can find us on Telegram, which all of you have already been doing Your questions honestly help everybody learn.

Appreciate you guys spending time with me listening through all of this. Hopefully it was valuable. We definitely appreciate your feedback. After you've given us all, listen let me know your thoughts and what additional content we need to address here so that you guys can keep moving on your privacy journey moving forward on your privacy journey.

Thank you. Have a great night.