Is it going...

Hey, it's wonderful. It's very sunny here today, how is it there for you?

Ah wonderful... Yeah, also I'm just outside of Warsaw So, and it's wonderful and Sunny was quite cloudy, but you can feel late summer.

[Carrie]: I love it. We have with us here today, Lukasz, and this podcast is part of the AXIS 2020 event that we've been having for the past month in August.

This program falls underneath the USABLE project with internews, and Lukasz had hosted one of our community-led sessions or skill share sessions, and we're happy to be able to share about his project today and some of the things that he's passionate about when it comes to digital security. So Welcome, Lukasz.

[Lukasz]: Thank you so much for inviting me here. It's such a pleasure and such an honor, thank you.

[Carrie]: Yes, Lukasz, can you tell us a little bit about who you are and what your background is and what you're currently thinking on and working on.

[Lukasz]: Sure, of course. So Hi, everybody, I'm Lukasz. I'm usually based... It's somewhere in Central Europe. So now, I'm usually traveling between Warsaw and Sariento, which both of the cities are absolutely wonderful. I'm currently in Warsaw and I'm really, really missing the hills of Sariento. By education by trade, if you could call it such, I'm a political scientist, and this allowed me to pivot a bit more and to think about security from a psychological and from a social perspective, and I've been doing and attending digital security trainings for quite a while already. And one of the things that I noticed was that whenever we were talking about specific tools, very often the lesson was, We're doing this tool, because the trainer told us to use this tool, and when I so started asking people around, Why are using this tool? Why using signal here? Why are you using WhatsApp, why are you using Telegram?

I feel that the most common reaction I got was because someone I trust told me to use this tool, and I think that that's fantastic, that people can rely on trusted sources, and people can rely on trusted friends, the issue is that such knowledge is not partially future-proof.

So VPN provider, which might be great in January, might no longer be a good option in August. A messaging app such as take secure, which was seen as the recommendation no longer exists and has an example being re-branded to Signal, and we don't know in which way. Let's say messaging app, such a signal, WhatsApp, a VPN service and a lot of other things will develop.

So I noticed that a lot of digital security training focused on giving people a really fantastic knowledge, but giving this knowledge in the moment, giving them the current state frozen as it is,

and I noticed that a lot of trainings weren't really focusing on figuring out in a couple of years from now, if we should use this product, service, or tool, and if it's product, service, or tool fits into our respective threat models, so I've sort of been doing a lot of work over how can we create something like could check lists, How can we create a simple list of rules to allow people to figure out if a current product is legitimate, good, or fits into their specific use case and threat model.

[Carrie]: Wonderful, thank you. So thank you, Lukasz. And for formalities, I will be hosting our podcast today. My name is Carrie Winfrey, I'm the founder and lead at Okthanks. We are an interaction design firm and have done much work on open source tools that are privacy-centric, so I'm super excited to be able to speak with you today, Lukasz, and just explore how some of the things we've been thinking about intersect. And you had mentioned having this very simple checklist equips people to assess tools to understand how secure they are. I think this is super important to empower people in this way, and also noting that these things do change from moment to moment, so it's important to be able to decide for yourself and really determine for yourself if something is safe to use, and if you can trust the people that are behind it.

So I would love to dive in and hear more about what the simple checklist is, what is it about, and how would someone use it. So I think Lukasz, if you would, take us into the scenario of how you would talk someone through assessing a tool...

[Lukasz]: Of course, with pleasure. So first of all, I think the first thing, and that's a very, very good friend of mine, helped figure this out when I was discussing the checklist with him initially. He said that most of the people we are training are already doing some sort of fascinating and deep research already, so most of the people we are training will be, for example, activists we've been pouring for tax records or journalists will, for example, be analyzing, investigating huge saves of data. And if we, for example, ask those people a question such as "is this financial institution legitimate?" or "is this local government report accurate?" they would instantly have an answer, but at the same time, there is something interesting happening with whenever we started to talk about digital security or digital tools in general. I think a lot of people feel that this was not practical for them. And for me, it's been... Technology has been sold to us, it's magic for a very, very long time, and technology has been sold to us as like the type of magic that we cannot touch, feel, open, or interrogate. And at the same time, I think that the types of people who we are working with, a lot of them already have these tools to look into and interrogate, almost any structure that they find. So one of the reasons why I did this in the form of a checklist was to empower people and reassure and that can make easy decisions about digital security, just like they can make easy decisions about lots of other factors in their lives, for example, whether you trust it's a certain institution, whether let's say a bank or financial institution, they investigate is legitimate, anything really.

[Carrie]: Wonderful. Yes, and I love that notion of really empowering people and so that they can be reassured and make an easy decision.

Digital security can sometimes feel very complex and complicated, and it is complex, so to have a way to make simple decisions really makes it accessible for everyday people who may not feel super tech-savvy, or who we tend to just shut down. And when it comes to being tasked with understanding if something is secure or not. So, yes, there's such value in this. I know in some of our work and research that we have done over the past year, we were trying to understand how

people decide how to trust apps and how they decide which app to download. We were diving in... We did multiple interviews in various parts of the world, and we wanted to understand the behaviors around getting apps, deciding which one they would choose, and this was all done on an understanding that there are fake apps or clones of apps that exist out there, in the world and in the marketplace. In some cases, this is actually having a bad effect for some tool teams that were working to develop open source tools, so that was the base of the research project. To tie back into what we're talking about now, we did hear a lot that if someone you trust tells you to use it, that's very quickly and easily permission to use it, you know.

[Lukasz]: Yeah, definitely, definitely. I think that that's a very, very good reason to use it as well.

[Carrie]: Yes, it is, yeah. Yeah, and we also found, however, though the person that was saying, "Oh yeah, you can trust us, you can use it," or that was sending you a link to download an app, they may not... They may not actually know they could have been handed a fake version of an app or one that it has malware in it.

So yes, it's good to be aware of both of these things, and I think to really emphasize the importance of the product in the work that you have done, empowering people and equipping them with their own way to like check-in and see is really important and critical in what we're doing. Would you like to walk us through, say, if a video conferencing has been such a huge topic in the midst of Covid and so many folks are having to shift from and shift what they're doing even more online or on online, completely... if they weren't doing their work that way before. So with video conferencing, there have been some things that have happened with Zoom and news has come out. Would you like to walk us through how you would assess Zoom today? And if it's something that you would feel has all of the security features that you would need in the context that you're working in.

[Lukasz]: Yes, of course, of course. Very quickly, though, you touched up on something really, really interesting also about a trusted friend who might be recommending an app and the trusted friend might still be giving you a fake version of the app, and I think that it's actually really important to distinguish social trust from technical trust.

So I think the technical trust is the trust the other person to do something very, very well or be very well-skilled in something, where social trust is trust on a very, very personal level.

So for example, let's say that I would have very, very high social trust towards my best friends, which means that I would probably trust them with my life, I would definitely trust them you know, with the keys to my house, with cat sitting, with anything, but there's no way I would trust them to something, for example, reliably remove my appendix, and I would definitely on implant, which I would definitely reliably trust a doctor to remove my appendix. I wouldn't probably now give the doctor who removed my appendix my house key and be like, Hey, I'm up for two weeks, can you please take care of my cat?

So I think that it's very, very important to realize that trust actually goes into many dimensions, and social trust and technical trust are two quite different things.

[Carrie]: That's a very good point. It seems in the medical world that line may be a little harder drawn then when it comes to recommending products or apps for people to use as well... You know what I mean? So there's a little cost.

Yeah, that line gets blurry, Depending, depending, quickly, depending on what it is before you... But I love that, yes.

[Lukasz]: Yeah, there are many, yes, and all... I'm always afraid of downloading a fake version of an app, so what I will usually do it is I will at least both open... If the app has a Wikipedia page, I would probably open it with a wikipedia page, I will then open a Google search for the app in case someone modified the Wikipedia page, and then maybe I will also check it an institution like the EFF or someone else linked to the app and only if two or three of the URLS are the same will I really, really trust the app, so I'm super, super fearful of fake apps as well.

[Carrie]: I love that process that you go through, it's very good.

We now have another mini checklist for what to do before you download an app.

[Lukasz]: Yeah, no, I mean, I love checklists because the world is so complicated and can get so absolutely overwhelming for me. For me, a checklist just means you sort of outsource your... a lot of your thinking and a lot of your memorization to a piece of paper, a piece of digital paper, and that's always so helpful for me because it means that you are not responsible. You don't have to stress about missing any of the elements.

[Carrie]: Yes, I would like that in my personal life to meal planning, if you know, if you have everything written down that you're having, you now have to come home and as the dinner question, what are we having for dinner tonight? We didn't thaw any meat out, oh no we're eating out.

But yeah, reducing the mental capacity that people have, that it requires to take, to figure it. Yes, reducing mental capacity is huge, and I love that also, that checklists do that for you.

[Lukasz]: Yes, exactly, exactly. And I think that one of the main items on the checklist for me is just to really check what do people you trust say about this product or app? Or the other thing is, so does this product or app make any misleading claims, so are there any controls is surrounding it? And I think that Zoom is an absolutely fascinating example of this, because with most services, what happens is that they build our trust, they build our trust, they build our trust, and then they do something that makes us lose our trust. So there was the wire messaging app, and I still use them quite a bit, but I think that they took, for example, new investors on board from new jurisdictions, and they took quite a long time to tell the users about the new investors, and I think that a lot of people are very upset that there was such a lack of transparency from the company that market itself as a security front, that's Wire.

But with Zoom, it was kind of the opposite.

So Zoom started off by growing very, very aggressively and actually doing a lot of security

missteps, so they would, for example, call themselves encrypted where they weren't really what most people would understand is encrypted, because they were only encrypting the communication from your computer to zoom servers rather than the communication that was passed around, if I remember correctly. So since Zoom was pretty much mis-selling, and for me, mis-selling was a huge huge red flag. And then they changed.

[Carrie]: And how did they change?

[Lukasz]: So one of the big things they did is they really went through and they really backed away from a lot of the security criticisms that they received after awhile, so they totally changed the cost, they... First of all, got really, really... They announced a feature freeze for a certain amount of time, which meant no adding of new features, just focusing on security, and I think that this was the first single of reliability. Then they became very, very transparent about the security features like waiting room stuff that they would integrate. And finally, I think one of the really important things that they did was they got a bunch of pretty reputable security professionals on board to serve sort of as consultants, and one of them was, for example, Alex Stamos who... He actually quit Facebook after disagreeing with the Facebook board position on Russian disinformation, essentially Alex is one of those people who, I think reputation is very, very important, and who definitely not want to destroy his reputation by being involved with a company that doesn't treat security seriously. So essentially, the fact that they hired someone for whom reputation was very important, and they managed to keep this person on probably meant that they are very, very serious about security, and the people who are starting to work with them are very, very serious about that as well.

[Carrie]: Yeah. Wow. Yeah, that's a great observation. Are there... I know within the checklist that you've developed, there are... You spoke a little bit to... Yeah, what do people say about the product? And your second point, has a product... Have the product claims ever been challenged in court? What are your observations? Related to zoom, on the second point.

[Lukasz]: So I'm afraid, I haven't been tracking the zoom or... So with a messaging app, it's a bit different because the main times that would be challenging the could be either claims for user logs or alternatively, things, for example, when VPN sharing Oslo and there haven't really been any super high profile court cases with regards to zoom yet. There have been cases where Zoom has bowed to some, not particularly, democratic government, and it's been a rightly criticized a lot for us, but in general, there haven't been any big demonstration called cases.

One of the reasons why I put it there, I put the cold case thing there is because I was fascinated in Signal's response about this.

So what happened once was that Signal was essentially taken to... There was a law enforcement request for data on a signal user and Signal only managed to give two pieces of data on this person- the last time they logged in and the moment at which the account was registered. Signal was not able to provide any other data, they were not able to provide any data on whom they used Signal to communicate with, they were not able to provide any data about content of the messages, they were not able to provide any data about the locations from which they were connecting or whatever... And this is the law enforcement request, right.

So essentially, if signal did not agree to provide this data or if they had lied about the type of data they had available, they would probably facing very, very serious legal consequences, probably including prison time depending on a jurisdiction.

So essentially, if Signal says that they don't have this data, that they cannot collect this data, and they do, so essentially it putting their own freedom of future organization as a guarantee, that's a pretty, pretty big green flag, and if, for example... And a lot of other VPN, lot of other apps, for example, VPNs have done this as well, right. So for example, there are vpns which have had cold cases against them, and they've actually been unable to get a user data because they haven't collected them.

So for me at watching what happens when there's a threat of legal action against the institution, it's one of the best ways of checking whether not or what data they log and how honest about the data they do log, because of course they have... In some VP and switch from is not to log, and the moment the police asks and suddenly the logs appear.

So another interesting thing for me are all of the congressional hearings above in the US and in other countries as well, of tech leaders, and essentially sometimes Congress will ask is, for example, if the company is able to access such and such communication or whether or not it's encrypted or not. And in some of those cases, the leaders will be talking on their oath or they will be facing criminal penalties for saying the wrong thing, so sensitive, for example, the CEO of an organization can testify under or a similar measure of these criminal penalties poling to Congress or in other government body, and they still say, we cannot access this, this is pretty encrypted that I think that that's a very, very good reason to trust them. Alternatively, they might be cooperating with the government on some sort of secret tribunal, but that's pretty unlikely. So I'd say that's a huge green flag and we can probably trust them.

[Carrie]: So your third item on the checklist is what data or permissions does the product require from you? It seems that there are some... You spoke about in court cases, it's often highly realized what a company like Signal actually knows about you when they're asked to give over data. Can you share with us about this kind of third point about what data permission does the product require and how you would actually go through and assess or know the truth about what the data that they're required from you?

[Lukasz]: Sure, of course. So I think that if they are products that have been designed from the ground up as privacy products, for example, very secure messengers, such a Signal, for example, VPNs- if they collect any more data than the basic sort of minimum thats instantly seen as slightly suspicious.

So, Zoom actually wasn't created as a security first product, Zoom was probably created as a quality first product, and this means that Zoom can usually collect a bit more data in most of the ports, but for example, signal collects next to no more data than your phone number, right? You don't, for example, need to sign up with both phone number and an email, if you did have to sign up with an email, that would be slightly sketchy, like Why are they trying to collect more data about you when they really need? And I've also been really interested in vpns and how a little data they can collect, so now about the Swedish-based VPN, for example, doesn't even identify you by email address,

they can just identify you buy a 16-digit code, and in all of those cases, if one collect that little data, it means that they are very, very well-designed, it means that they are essentially... They've taken a long run time to think about the design, to make sure that as private as possible. If in the worst case scenario, such a company would get breached or have, for example, law enforcement request, it means that there would be very, very little data that they could collect about you in the first place, or that they could reveal about you in the first place, so I think that if you, for example, put your sensitive communications in a company that in no way to... Into your real life identity, this means that even if the company were for example, breached and let's say some metadata would leak, they would not be able to tie back to you. This is also why, for example, the requirement for services like signal or what's up to require your real phone number can be so controversial, based in a lot of jurisdictions, you cannot really get an anonymous phone number easily, you do, for example, to register your phone number with your ID card or passport. So essentially, theoretically law enforcement authorities, know who is behind every phone number, which means that if you are in a less than Democratic jurisdiction, it means it sort of corrupt police officers could easily figure out which real life identity stands behind which person in a Signal group, for example.

So even stuff like phone numbers could be very controversial to collect. I know that the Signal team has just totally tried to justify it very, very well, that they need the phone numbers because that's the easy way in, but people can find each other, et cetera, et cetera, and they are working on a way beyond this, but for me, for example, if Signal would no longer require any phone numbers and move to use names as they apply to do soon, that would also be a huge, huge green flag.

[Carrie]: Could you help me understand... I'm thinking about an end user or an individual that may identify themselves as non-tech-savvy and kind of new to digital identity and what that actually means. What advice would you give to someone who is kind of looking at tools and saying, Okay, I know that I need to think about the personal information they are collecting on me... what advice would you give them to help navigate how you know if an email is okay or if a phone number is okay, versus other methods? In thinking at a very raw level, there are standards that are set, right? So in a lot of messaging apps, require your phone number, and it seems that for some people it's like, Well, it's so normal that you don't have it and really think about it, but you talked about the implication of in many places, like your phone number is connected to, it's registered with your ID in your country, so it's highly tied to who you are and what other information your government may know about you because of that, but yeah, at a very raw level, what advice would you give to someone who's new to this kind of thinking to understand what is okay to give away in regard to their personal identity?

[Lukasz]: I mean, that's an excellent question, and I would say that in most cases, would probably need to ask the person themselves for a very, very simple reason with that. We as digital security trainers cannot know what's happening in every situation or every jurisdiction, and sometimes a large part of our job is just listening to people. Right, so if we were, for example, asking journalists or activists from a Not particularly democratic state, they would probably know much, much better what sort of data can easily be traced back and what cannot, and then I think sort of they will usually know much better. For example, if the government ever relies on phone IDs or not, they would know much, much better about those sorts of things, so it kind of reminds me of the old joke that in countries that were once occupied by Soviet authoritarianism, you would sometimes start a phone call by saying "Hello. Let's say hello Carrie. Oh, and also, hello to the colonel who's listening

into a phone call... I hope the colonel is having a good day as well."

So I think that there's a lot of those.

So I think that in a lot of those places, so of knowledge of surveillance has been very, very pervasive, and very often people will know much, much better on the ground, so I don't want to step into... Step into places where people... My training have much much better on the ground knowledge than I do. But in general, I would say that sort of be wary sometimes of your phone number unless you can easily get anonymous sim cards. I would probably show people how to use an easily disposable email address, and I would probably also show people that sometimes it's reasonably easy to register services that don't track you, or they actually a business model that don't track you, 'cause sometimes if I would talk about services like duck duck go... And I think that this can also extend to services that give, for example, disposable email addresses, in a lot of those cases, people just find it difficult to believe really, that those services don't track you because they were so used to tracking and data collection is a pervasive intimate data model.

So I think that giving people the confidence to see that actually some businesses or some organizations are built in the model that doesn't include tracking and just even hinting at this and telling them, You know, trust me, this is the case, can go a very, very long way.

[Carrie]: Yes, that's a wonderful point.

I want to skip- We're not skipping, we're moving to the 04 on the checklist, which is related to location, so whereas a product and its developers based, would You so kindly tell us about why this matters and what the considerations are?

[Lukasz]: Yeah, of course, I think that jurisdiction is one of those things that can be kind of important, and I think that its importance cannot be over-exaggerated either, so in many cases, you probably want your product to be being a reasonably legally stable jurisdiction or for example, if your threat model comes from the types of people who are based in the country, that your product is done in, you probably shouldn't do this right, you probably shouldn't be using the... So for example, let's say your threat model is Russian secret services, you probably shouldn't be using products that are based in Russia. Just because Russian secret services could, for example, have some sort of way of, let's say, for example, threatening or threatening to arrest the tones of the product, of course, into giving up data on you, you are much, much better off in using product based in jurisdictions that are much over outside of your area. That this is really, really important as a starting part, and I would say in most cases, you should probably look at products that come from jurisdictions that you would consider to be reasonably democratically and politically stable, so I think that in a lot of those cases, there's always a risk that the police or someone could come and knock on the doors of the product developers and as it of example, building a back door and the stronger democratic system in the country, the more oversight are over police forces and... Or intelligence services, the less likely it is to happen.

So once again, this is a very, very local decision, and I think that I would definitely want to ask activists on the ground and journalists on the ground about it as well, Do you... For example, they think you're using a mail service that's based in the country, one of the first questions that I was

asking is, do you trust your countries, for example, security services not to coerce your mail for, let's say, your communication details of metadata.

[Carrie]" Yes, I went in to highlight as well, you brought up a couple of times how important is to ask the people within their local context, because they are often very knowledgeable about these things and what... About the jurisdiction itself, I wanted to hit that we have within our access convenience over the past month, we have seen this, we've seen this first-hand, and being able to connect with so many folks across the world who are working very hard and diligently within their communities, we have seen that knowledge and it is there, and there are people... I would say even if you live in a particular context thing, you don't feel that you know all the things that you need to about your jurisdiction, there are certainly people within your community that do have that knowledge.

Alright, everything that you've shared has been super insightful with the checklist, [Thank you so much]. Yes, of course, there are many more considerations included, which I would love to go over all of them, but there's one specifically that I wanna make sure we have it before we wrap up our podcast for today. And that is open source. Could you tell us about why this is on the lesson... Why it's so important?

[Lukasz]: So first of all, I'm sure that this podcast, given the fact that it's a very open source complex, will definitely be very, very biased towards open source, and I'm super biased with open source and almost all of my security tools as well, so essentially, if it's open source it means that the code is pretty available for anyone and anyone can really read it, study it or relax now, in theory, this means that everybody can look for the code and read it in the Spain practice. Unfortunately, it means that it's mostly restricted to people who know coding and computer science really, really well, and unfortunately, we've also had some pretty nasty bugs, errors and back doors and open source software, so just because the software is up online and everyone can read it, it doesn't necessarily mean that it's free of bugs, but it means that people can generally take a look at it and vouch for its accuracy and vouch, but it says what it does, and this is really, really important, especially if someone's on a new product or a more niche product.

So one of my favorite examples about this is Objective-SEE. He saves a suite of security products from MacOS, it's done by Patrick water, who's considered one of the formal experts in micro security, but honestly, very often when I see a security product and slightly slightly skeptical, 'cause if there's one way I could gather the data to all the types of people who are paranoid, required encryption and have elevated security needs, it would be by in she publishing a security product and letting it to contain a backdoor that rather than protecting your data actually picks... Or if you think that... So essentially, for me, security conscious people can actually be much, much more vulnerable because they get a lot of sensitive data and deal with the sensitive data. So Patrick Waters did produce almost all of the source color, all of the source code for Objective-SEE tools up online, which essentially is that any security expert or even most advanced coders can just look at the code and see that it does what it claims to do, that it doesn't excite any data from your computer, but it doesn't contain any nasty factors, but it didn't tell us what it has... What it has to do and what it's been designed and was being lit, and this in itself... This is huge green flag.

Now, I think that we sometimes overstate the capabilities of open source software, just be

something as open source does not necessarily mean that it's 100% secure and anyone can instantly find security bugs in it. Some security bugs are very, very nasty and very difficult to find and prideful to be, but in general, it's... At least it could guarantee that the software doesn't take any of your data that doesn't contain any particularly nasty malware, that it doesn't try to still excite anything insured into a guarantee, but it does what it came to do, and it does what it says on the box.

Now, there's something even more complicated with open soft, which is called reproducible builds, and I don't get into that in a huge depth, but essentially there's always the question of how do we actually know that the app that we download, let's say on a phone or a computer, it's the same version of the app, which has the source crept up on, let's say, a website like GitHub, and this can be sometimes difficult to determine very... Ask them them very clever cryptographic ways of doing it, and Telegram, the messenger has been pushing, if I remember correctly, quite heavily into reproducible build, and so doing this... So usually would not open source software, you can have to trust the company about the contents of the software and you have to trust its claims, so with what's up, which I'm still a fan of, in part of everything, you have to trust Facebook that... What updates, what Facebook claims it does was with a lot of the Airsoft with telegram and which signal you can look at much of the sole code and verify for yourself, and that's really, really powerful, especially for startup apps, Monica and especially for products. Target towards security professionals. Because part of me is always people that product target to do IT security professionals have potential to just be a Honeypot, collect everyone who has sensitive data and gathers and exotics data.

[Carrie]: Yes, I wanna ask a similar question that I had before about this, if, again, if I am non-tech savvy and I'm looking at an APS website or products website, and at the end, it's like, we're open source, and that is awesome and great. From that statement, how assured can I be that the due diligence has been done that someone that knows what they're doing, a security expert or someone more tech-savvy than myself has gone in and check the code and make sure that there isn't a terrible malware and that the code is truly honest.

[Lukasz]: That's a fantastic question. So I think that one of the things that we could definitely do in our training is to, for example, show people... Let's say the content of GitHub, I mentioned get humor, and it's a place where people... Or get land as well, voles, where people send through their contributions to open so software and both of both our places where people can sort of see how many people contributed to it, how big is the group designing it? Is it a single person? Do they receive a lot of feedback? But that I think other bigger projects, for example, Linux have very, very well-documented commits, but they aren't particularly the code politics, let's say, Didn't particularly beginner friendly... And I think that the last thing is that the bigger, more prominent are more popular open source at the higher of arcane, but more and more people have looked at it, right.

So if, for example, I were to create locations super encrypted messenger tomorrow, and I was the only contributor and all of the code appear on get GitHub overnight, that's kind of sketchy, but if we, for example, looking at something like... For example, signal, there are lots and lots of security professionals doing all this up signal, they lost a lot of security professionals write thing about Signal, and in most of those cases, they have expressed very, very positive opinions, so it in itself is something that's really, really important and espouses... Well, I think the open source allows universities, professional companies to start the forming, reading deep and fascinating audits and

analysis of it.

Sometimes the results are great.

Sometimes, for example, telegrams-crypto has been critiqued quite a bit, but the verified that telegrams-crypto has been very openly documented that all of the source code for the crypto is available. This in itself has been a huge, huge green flag as well.

[Carrie]: Thank you for unpacking that a bit more for us. Lukasz, it has been a pleasure to have time with you, I love your eagerness and excitement to dive into all kinds of topics actually, but it's been lovely to have this time today, and for those that are interested, Lukasz does have the information in the checklist published on his website, so it is accessible and available to use, and as I understand, if anyone is interested in collaborating on it or giving input is... They're very open to that.

[Lukasz]: Yes, I would love to. I really love some crowd sourced digital security projects, and I'm always trying to find more projects and bigger list and essentially, especially checked, 'cause I think that there are a lot of really cool guys, I'm slightly obsessed with checklists just because I think that organizations very often, have very, very few easy and straight forward checklist processes that they can... So I'm always keen to work with you.

[Carrie]: Awesome, thank you so much. Perfect, thank you so much for having me.