Rachid Finge (00:01):

Hey there, and welcome to the Made by Google Podcast. I'm your host, Rashid Finge, and this is the podcast where we take you backstage at Google and get the insights from the folks who built the products you use and love. Now, this week is all about security. What does Google do to keep users safe, especially on mobile phones, you have that thing on you all the time. So keeping it secure is extremely important. What is the biggest threat these days? And also, where does Google's job on security end? And where does yours as a user start Discussing all these topics today with someone who is a top expert on the topic. He's the director of Android Security Strategy. Please say hi to Eugene Liderman. Eugene, welcome to the Made by Google Podcast. Please tell us a bit more about your role and how you ended up at Google.

Eugene Liderman (01:02):

Yeah, thank you. So I've been here almost five years. It'll be five years in April. I'm the director of Android security strategy. Primarily, I focus on external evangelism. My team participates in a lot of security standards, right? And we do a lot of certification work of our products and help our partners certify their products to help build trust. Prior to Google, I was at VMware for a couple years. And prior to that I was actually at a company called Good Technology. I've worn every hat you can think of. I've been in product management, product marketing. I've even had a couple stints working for the government. So what's really neat is I started my career kind of working on more backend infrastructure, pre-cloud, right? So more of sure traditional IT information systems. And as I've a evolved in my career, it's kind of moved from cloud to mobile down to now at this point, the mobile OS.

Rachid Finge (01:47):

Great. Now listeners of the Made by Google Podcast know that I usually go to the internal directory of Google, you know, where I see the personal mission statements of people. Yours is the longest one we had today. I think it had like a length limit in the past, but we let go of that and you made sure you use that. It says build trust with consumers, developers our OEM partners, KOP informers and Enterprises around Android security and privacy capabilities through outreach, transparency and independent validation. I guess that basically covers everything. There's nothing left out there, right?

Eugene Liderman (02:21):

Exactly. It's comprehensive. I think

Rachid Finge (02:23):

Today's guest has dedicated his career to cybersecurity. Eugene Leman has been fighting the good fight on all levels and on all sorts of computers, cloud ones, virtual ones, and now mobile ones at Google. As a director of security strategy, it's his job to make sure Google does the right things to make sure all Android users are well protected. That goes from things you might see, like Google play, protect to things you don't like encryption. And as you'll hear, working on security at Google means making sure you as a user can enjoy the nice things while Eugene does the heavy security lifting for you. Just don't ignore those red lights. I hope you'll enjoy our conversation. So let's start our discussion with transparency, because maybe that's not the first word you kind of think about when you think about security. So why is transparency important to keep people safe?

Eugene Liderman (03:25):

First and foremost, transparency builds trust. I mean, in any relationship you have with other people, being transparent is a good thing. I actually apply that in my own personal life. I try to be very transparent with my wife, my kids, sure. And everybody else doesn't mean I come off rude. I try to be nice. But I definitely try to be transparent. A really good quote actually comes from the Dalai Lama a lack of transparency, results in a distrust and a deep sense of insecurity. So it's something that we just try to abide by.

Rachid Finge (03:48):

That's a good point. And you're right, that that's not only for personal relationships, but I guess being transparent in how we treat people's data or the things we do to keep that data safe. People will want to know about it.

Eugene Liderman (04:00):

Yeah. The other big thing is, I mean, as you know, Android is open source. That's a really big factor for transparency. If anybody wanted to, they can simply review the changes that are being made. Actually, it helps us work really closely with the research community. We publish a lot of content. We even publish a quarterly transparency report that has topline metrics for things like malware and device updates. And we're always trying to provide more information to all of these target audiences that I mentioned above. Right? So it's consumers, key opinion forms, developers, OEM partners.

Rachid Finge (04:28):

So, you know, that open source side of Android always confuses me a little bit because, you know, on one hand of course, people can see if, you know, that is the ultimate form of transparency. I guess at the same time, if you're a bad guy, you can probably figure out, you know, whereas Android's weakness and then exploit that. So how do we keep that in check?

Eugene Liderman (04:47):

Honestly, the way I look at it is the fact that it's open source means we have a lot more people protecting Android, right? When you're running a proprietary closed source system there's not a lot of eyes on it. It's kind of hard to scrutinize. It's a lot of people refer to as security through security. You know, transparency does shine a light, but that light means we have more people looking at it and partners protecting. So that means security researchers, academia, other security companies, you know, everybody's trying to do the right thing and protect the user. And so if you actually look at some of the high benchmarks when it comes to security, especially on mobile, enter Android devices achieve some of the highest ratings. We've gone through a lot of Android devices are approved for military use in the US and other countries. So I mean, it, it doesn't hold it back at all. I think it actually strengthens it.

Rachid Finge (05:31):

So we're now talking about the lower levels of security as it's often cold. We know we're talking about the operating system, basically the hardware. What are some of the things people should be aware about when they think about their security specifically for mobile devices?

Eugene Liderman (05:46):

Yeah. smartphone technology has evolved greatly over the years. I mean, there's a lot of things I would call below the surface. The user never sees they're just there and running. You know, obviously devices have encryption that, that encryption usually, usually hardware backed right on these devices. Not to go

super technical, but there's usually a hardware root of trust and that is used for key primitives, like generating encryption keys for the entire device, protecting your biometric secrets when you use to authenticate to the device, ensuring that the integrity of the operating system is there. And as you kind of move up the stack, the OS does a lot as well. Right? So the os isolates everything. So, you know, everybody talks about app sandboxing as a good example. Sandboxing basically means that every single app in process is isolated from one another. You know, it has its own dedicated CPU cycles, access to memory, access to storage. And the only way it really communicates with the system is through permissions. And then it can communicate with other apps as well. But it's all isolated in a way. So that kind of guarantees everything is separate from one

Rachid Finge (06:41):

Another. Right. So if one app runs into trouble security or otherwise, it won't affect another app.

Eugene Liderman (06:46):

That's the general goal of it. Exactly.

Rachid Finge (06:48):

Right. Okay. So you were talking about things we don't see, maybe something that we do see as a user, if we sort of move up the stack to keep people safe. Is Google Play Protect, maybe users, you know, of course they know Google Play, that's where they get their apps from. But what is Play Protect and how does it work?

Eugene Liderman (07:05):

Play Protect is the most widely deployed anti-malware solution. It's installed on over three and a half billion devices. Wow. It scans over 125 billion apps every single day. And that formulas, basically, if you take the number of devices, multiply that by the number of apps they have on the phone, it does a daily scan of all those apps. It's both an app on the phone, but it's also a whole backend infrastructure. So every app that gets submitted into play goes and gets scanned through Play Protect. It does a bunch of things. There's static analysis, dynamic analysis. It uses a lot of machine learning to analyze patterns and so forth to see what's going on with these apps as they're submitted. There's heuristics, signature checks, heat maps, the user doesn't know that because when they go to the Play Store, they install an app, the last thing they'll say is, oh, scan, you know, scan by Play Protect, and then it downloads it to device. Now that's just before it ever gets submitted into play. Of course, it also, as a user, you have an app on the phone Play Protect service rather. And you can get to it from the Play store or from the settings of the phone. And you can always run a manual scan. It works offline as well. And it basically will show you that, you know, you have no malicious apps on your phone. It also actually scans if you do side load or download outside of the Play Store, it will scan those as well on your device. So it's, it's fairly comprehensive.

Rachid Finge (08:20):

Now, you mentioned machine learning in your answer machine learning ai, two topics we talk a lot about on this podcast. So how is that beneficial to something like Play Protect?

Eugene Liderman (08:30):

Yeah, I mean, anything that you wanna do at scale, right? You're gonna be leveraging machine learning and you, you kind of hear this across the board. I mean, obviously I know it's, it's very popular now

because of what we're talking about with chatbots and everything else, but But overall, I mean, it's, it's been used in security products for, for a long period of time. It's used across all of our product suites, right? We're always using machine learning and training in various models to understand, to be able to pick things up at scale and, and detect. And so this is not just a play protecting actually it applies to what we do for anti phishing as a good example across all of our first party apps as well.

Rachid Finge (09:01):

Well, let's talk about Phish, because that is definitely a topic I think people are worried about. It's maybe one of the larger threats, if not the larger. Is it perhaps the largest threat you could face on a mobile phone?

Eugene Liderman (09:12):

Honestly, I think at this point, Phishing has overtaken malware, especially during covid. It went really bad. I think Phishing spiked heavily, and this was, there's lots of research that it was across even enterprise and consumers. In fact, there was a study cited by C N B C that said in 2022, Phish on mobile went up like 50% phish and identity theft or attempts. And the reason for that is because if you look at a traditional legacy medium for phishing, it'd be your laptop or your desktop. Okay, well, you're connected for a little bit of time. You put it away, your phone, you're always connected on your phone. Your phone's always, at least in my case, it's always in my pocket or next to me. And so you're going to get a message, you're going to open it and see that message and res and try to respond into something with it. Now a phone is also a much smaller surface. So as a screen, it's a little bit harder to discern if it's a phish message, right? You have to really read through it. And, and so I think this is why it's become such an important area to focus on.

Rachid Finge (10:05):

So how do we do that? I guess? So phishing is maybe someone sent you a link, you click it, maybe you shouldn't have done that, and then we sort of got to make sure nothing bad happens. So how do we approach that?

Eugene Liderman (10:17):

Let's start with like, what is, like you said, what is Phish? Well, phishing could be, you know, a way to try to, could fool a user into getting something out of them, or for them to do something that could be sending a link to install malware, if you remember, like flu bot, making them think that they have to log into a website and put in their username and password, right? And steal their credentials. I think the cool thing that we provide on Android is this out-of-box protection. So historically it was all email based. A lot of people would get Phish emails. Well, Gmail blocks 99.9% of those. And I think it, the latest stat that we talk about is it's like 10 million every second that we block in terms of scam. Wow. Talk about scale, right? Powered by ML and AI. But a lot of those Phish attempts have moved to text-based, right? So with Google messages, we actually also have built-in scam and phishing protection. And so what the way that works is it looks at basically the reputation of the sender, the reputation of the URL that the sender might send. And actually it's using ML to look at the patterns of the message itself to understand if it's a suspicious message and it'll flag it. And what's really nice about the way it works is it makes it really easy for the user not to have to worry, because as it starts detecting it, they'll start moving it to a out of your inbox, out of sight, out of mind. You don't have to sit there and freak out and be like, is this an important message or not? And some other operating systems have a much more blunt approach of saying, let me just block all unknown senders.

Eugene Liderman (11:38):

Well, what happens in that situation? What if you get a text from your pharmacy or from your doctor, or a one-time passcode being sent to you? You might miss all of that important information. So you want to have a good balance there. The same honestly applies to voice-based, right? Like message based is popular, but voice based phish is also coming back. And so there's lots of great deterrents there with dialer, right? You have caller ID and spam protection. And then one of my favorite features not available everywhere, but I love call screen because at the end of the day, you know the people that run these Phish campaigns, they're a sales organization. They have quotas, they buy leads. And so if you can deter them, time is money. So call screen is a great deterrent because it kind of stretches that conversation out.

Rachid Finge (12:19):

And call screen is where, where just, just to be sure, call screen is where the Google Assistant answers the phone on your behalf first, right?

Eugene Liderman (12:24):

Yes, exactly. And it's done in a privacy preserving way. The last thing I want to is it's really all about layered security. So let's just use the messages example. I get a text message, it's a efficient link. As a user, we're so used to seeing warnings. We ignore warnings, right? Sometimes at least some users And so you see the red warning, it says, don't click this, this is bad user ignores that warning clicks it, it opens up Chrome. What Chrome leverages safe browsing, which is also leveraged across 5 billion devices. And with safe browsing, it will actually also detect in malicious websites. So then when that link is open in Chrome, you'll see this big red warning as well saying, Hey, don't click this. Right? But let's take it even a step further and say they did ignore that warning too, and they click it. Chrome will of course warn them not to download anything malicious. And let's say in this case, they install, they try to get prompted to install malware, well then that's when Google Play Protect kicks in, right? So it's really this kind of layered security approach

Rachid Finge (13:12):

That's a lot of layers. And that all starts in this case with messages where I wasn't actually aware of it, but there is, like you have in Gmail, a a spam folder with text messages that you probably have never seen and for good reason. But even if you would see it, you would click on the link, you would maybe open Chrome safe browsing, which basically is a very, very, very long list of websites that you know, no normal person should want to go to. And then even if you still get there, well you need to go to a great length to get malware on your device through this way.

Eugene Liderman (13:48):

And, and one other thing that just deletes it back to like, so like I said, is Phishing either makes you try to install something bad to compromise your device, or in this case, try to steal information from you And so I think this is another great example where if you look at all the identity protection features that you have on your phone that are powered by Google, really, right? So a good example, one is password manager, right? So the fact that you do have the ability to generate and store passwords, and it'll actually alert you if any of your passwords have been compromised. The other thing that you have is because your Gmail account's so important to everything you do, one, you can protect it using two-step verification. Sure. You can get a one-time passcode, or my favorite feature is phone is security key, where I actually use my phone as a physical security key, and that that is impervious to Phishing attacks. And

then the last piece is you have this account and security checkup feature. So literally if somebody ever tries to log in as you from anywhere, you'll get a popup on your phone, let notifying you can see all your recent activity in terms of logins from where they happened. You can revoke access right away. It really gives you that central place. And it actually all ties together because if you look at on Pixel devices and now on other Android phones, we have really unified the security and privacy settings on the phone And so you can see all of that in one place. And it gives you this really nice, simple kind of green, yellow, red view of what your cybersecurity hygiene looks like on your phone. You don't need to be an expert. You just see that information and then you can actually see that information directly from the notification center as well as a quick AI action. So you know, oh, hey, you have a password, but that you need to potentially change because it's on the dark web somewhere. Okay, cool. I did that. My status is green and I feel good Again,

Rachid Finge (15:22):

I think I'm green, I'm not green, I'm orange. I got to do something after, after our conversation. Yeah, that's interesting. So yeah, that's the security center in your Google account. Definitely worth checking out as I just found out actually something definitely that I needed to do. You just mentioned something that I find so interesting is, so sometimes we see that in news once in a while, a website, there's a leak and passwords leak, and then they are in the hands of criminals. And if you reuse your password on multiple websites, that could be pretty dangerous, right? Because those criminals could have access to other websites. You mentioned that Chrome or Google will notify you in a case such a thing happens. So how does that work and where do I get that notification?

Eugene Liderman (16:07):

Yeah, it's actually built in. So without going into the weeds, just think that it's, it's basically monitoring all the passwords. I mean, generally it uses the hashes of the passwords obviously to, to check for the passwords. But the way it'll work is it monitors that. And there's a couple ways that you can get access to it, but the easiest is through the security and privacy settings and that notification center where it just automatically tells you, and that's in your example, that's why it's orange. It's saying, it's saying likely you have one password that's been on one of these lists because there's always these dumps of compromised passwords and it's on the list and it'll remedy for you to change it. The other cool thing that I think you'll see a lot over the next couple years, especially because it launched last year, is the use of pass keys, which is moving away from passwords, right? There's this new password list technology, right. Using a Fido standard and public key infrastructure. And so, you know, you'll see I think a lot of more apps on phones starting to move away and all the major operating systems have announced support for Password

Rachid Finge (16:59):

So that is, I create an account with maybe a social media network and I just use my fingerprint for example. That's

Eugene Liderman (17:05):

Right. Under the hood there's more, but as a user that's all you kind of see. Exactly. And it's transferrable across devices and everything.

Rachid Finge (17:11):

Okay. And, and I've never been asked then to come up with a password in the first place and store it somewhere.

Eugene Liderman (17:17):

But until there's better adoption of that, I think, you know, leveraging, for example, your Google, Google identity for single sign on to other services and ensuring that your Google identity has two-step verification and better than sending yourself a text message. I think that's probably, you know, use the Google Authenticator app or like I said, use phone as a security key, which is a really, really cool feature.

Rachid Finge (17:38):

And then of course you also have these like almost actual keys that you put on your, on your key chain.

Eugene Liderman (17:43):

Yes. Well that's the thing. Phone and security key is using the same Fido U2F standard, but it's relying on the hardware of your phone instead of having to pay and carry a physical key. So I have one of those, I have a physical key, I have a couple sitting in my home, but my phone is my security key. So anytime I'm gonna go, it's just I use my phone.

Rachid Finge (18:00):

So this is almost more of a philosophical question, but if you look at security keeping user safe, if a user then gets into trouble, do you feel, is it like on the, on the industry or is that a user's fault?

Eugene Liderman (18:15):

We wanna make it as easy for users as possible. So I think the thing that we do, we provide really good out-of-the-box security, right? So we have all these services running outta the box to protect the user. Of course users can ignore lots of those things. They introduce their own risk So there's, I think there's a relationship there and a balance. And the one thing I would recommend to users is one, leverage all of these things. And two, you know, try to read up on some of the, the tips and tricks in terms of, you know we make it easy for you. Obviously password manager will recommend a new password for every single website that you set up an account for. Do that. Don't, don't go against the grain and try to say, oh, I'm gonna use the same password. Right? Or, you know, if you get an alert, make sure you're actionable. It's kind of like going to the doctor I think to some degree, if you linger and you don't take care of issues that are early, you might be much more sick. But if you follow the guidance in the security and privacy setting, so for you, you have that orange, you should act on it before it turns red.

Rachid Finge (19:09):

Definitely. That's a very good analogy. Yeah. Let's make it all green in the next hour or so. So Eugene, we close every episode with a top tip for our listeners. Something they can do immediately, maybe in this case to become more safe. I have a sneaky suspicion which direction this is going to, but please enlighten us. What's the top tip for our listeners this week?

Eugene Liderman (19:35):

Yeah, I mean I think I gave it away already. I should have saved it for the ending. But I definitely think that just leveraging what's available on these devices, so, you know, I highly encourage making sure that you have a scam protection turned on and Google messages leverage things like call screen and dialer and

caller ID and spam protection, which they're on by default by the way. So, and then if you see a red warning, red means stop, doesn't mean go. So definitely follow the warnings that you see on your device and leverage the security and privacy settings section on your phone if it's available to you. Like I said, it's available on Pixel, a bunch of other devices already and hopefully rolls out to more devices over time. But if not, you know, obviously you can still go to the settings page and see that. Also, there's other cool features like privacy dashboard. If you wanna know what apps are doing on your phone in terms of like what, what they're having access to in terms of permissions, you have that available as well. So just kind of be astute of what's going on on your device. And it's a team battle, right? We're we as Android and Google are here to protect, but the user has to do their part as well.

Rachid Finge (20:37):

Yeah. And it sounds like you do all the heavy lifting, so all the user has to do is not ignore red warnings and everyone will live a better day it sounds like.

Eugene Liderman (20:46):

Exactly. I think that's the, the thing to think about is if we do our job really well and make security not scary and kind of leave it just a couple decisions to you, you should enjoy your phone for all the cool stuff, like taking great pictures and watching videos and enjoying all the fun things you can do on your phone. Don't worry about all the scary cybersecurity stuff because we have your back.

Rachid Finge (21:06):

Well, we're glad we have you to have our backs and make sure Android and all those phones are kept safe in all the Google accounts as well. Eugene, thank you so much for joining the Made by Google podcast today.

Eugene Liderman (21:16):

Thank you. It's a pleasure.

Rachid Finge (21:19):

Well, I hope you are doing what I'm doing and that's doing the security checkup in your Google account or on your mobile phone just to make sure everything is all green. And all right, love hearing from Eugene how much work we do to keep you safe and how we use multiple layers of defense. So nothing is left to chance. I'm so grateful you joined us for this episode of The Made by Google Podcast. If you're not a subscriber yet, maybe this is a good time to make a change. Just hit subscriber, follow whatever it's called in your podcast app and make sure you don't miss another episode of the Made by Google podcast. Thanks again for listening. Take care. Talk to you next week.