Barclay Damon Live Presents *Cyber Sip™*
Season 3, Episode 5: "Keeping Kids Safe Online: A Call to Action," With Arun Vishwanath

Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Arun Vishwanath is back with us on Cyber Sip. Arun is chief technologist of Avant Research Group, which is a strategic market research consulting firm. He is also associate professor of communications at the University of Buffalo, one of the foremost experts in what we call the "people problem" of cybersecurity. And last but not least, author of the book "The Weakest Link: How to Diagnose, Detect, and Defend Users From Phishing," published by MIT Press. Arun, welcome back.

[Arun Vishwanath]: Hey, Kevin, it's great to be here. I got a lot of more things to add to that list... we started. We have a new startup called the Cyber Hygiene Academy, and that's basically focused on some of the stuff we're going to talk about today, which is...

[Kevin]: Yes...

[Arun]: Fighting what the school system is not. Cyber hygiene for children. So we'll talk about that in a bit, too. But it's great.

[Kevin]: That sounds great. No, absolutely. So your piece in Dark Reading is what led us to our second episode together called "Safeguarding our Children's Digital Future, A Call to Action." And just to set the stage here, we really do need a call to action. So looking through your piece and some of the support you have: in 2022 alone, 1,436 separate schools and colleges fell victim to cyberattacks. Those were attacks involving more than one million students. One of the more infamous attacks I think we're going to talk about is the Clark County Schools attack in Las Vegas, where parents know that their children's data might or might not have been accessed, and they're just not getting any answers from the school district. So first things first, why are schools such frequent victims of cyberattacks?

[Arun]: Well, you know, there's a couple of systemic problems, right? I mean, the first being that these are older technologies that most of these schools utilize. Right? We have not funded schools when it comes to technology to the rate at which we need to. So a lot of them are using older technologies and also legacy systems, legacy software. That's just one systemic problem, right. The second problem, and this is the real issue here, is they just don't have the skills in IT security to protect these systems. So you have archaic systems in one end, and you just don't have IT security depth to protect them. Keep in mind, you know, the best organizations out there get hacked. Imagine these school systems which are now locally funded, regionally funded, state funded, city funded.

[Kevin]: Mm hmm.

[Arun]: They don't have the resources. We're not paying people enough in IT security for these kind of areas, and there aren't enough people doing it. So it's a low hanging fruit when it comes to attacks. And this is why, you know, we talked about you mentioned the Clark County School attack. I mean, just as that attack was going on, which was late and that was the second time they got attacked last year.

[Kevin]: Right.

[Arun]: So they get multiple attacks. They don't learn from it. There was a concurrent attack going on in California in a couple of school districts over there. Using essentially the same ransomware. That's when, you know, you got a systemic problem where it's just spreading, no one's hearing about it. Victims don't find out nothing's done about it. And it happens again and again and again.

[Kevin]: You have not only lagging skills on the part of the school districts themselves, Arun, but you also have ever-evolving tactics on the part of the threat actors to so that the chasm between expertise, preventability. It's just growing. It's making it more likely that we're going to see more attacks in the near future.

[Arun]: That's a great point, Kevin. And, you know, think about it this way. There's an upward cascade in cyberattacks because the technology evolves. But compare it. So when you look at the baseline rates of cyber incursions and compare it with the baseline rates of regular crime, what used to be "old school crime," you notice that old school crime has actually gone down. If you look at the FBI statistics, cyber crime is on an upward trend and it's remained in an upward trend. And to your point, think of home security systems. They have not evolved in the last 25 years. You can have a home security system and they're not going to....No one knows how to hack that to break into your house. But cyberattacks are constantly evolving. So you're right, it's an upward cascade. By the time last year in Blackhat, we had a paper talking about how to use AI generative to create phishing attacks. Those attacks were already in the marketplace using.

[Kevin]: Yeah, and as you say, just think about the numbers. So when we talk about the metaphor of someone breaking into your home, which is useful, but in the cyber world, it's as though someone's breaking into your home or trying to every second we've....

[Arun]: ...someone the worst part of it. It's even worse, right? Kevin, someone's already broken in.

[Kevin]: Right. Right.

[Arun]: Which is insane to think about, right, Kevin? Yes. By now you, me, everyone in our household has had some data stolen from them.

[Kevin]: We have.

[Arun]: We've all received some credit monitoring service from some companies that we didn't even know existed in some firm out there saying, oh, your data was compromised in some attack, but you were not directly responsible for.

[Kevin]: Yes. And there's an exhaustion factor that applies as well. There are so many of us, and yet we get these class action notices in the mail and you can opt in. And here's credit monitoring. And statistically, 99% of us ignore those things because we're so exhausted. Or we assume that, as you say, our data has already been... it's already been stolen. It's out there. There's nothing I can do. And that's very dangerous. And we're going to bring it into the children's context because I think with children, even as I think the paradigm, as I like to call it, the paradigm is shifting from a focus chiefly on data security to an emerging focus on privacy. We have the next generations that do not guard their privacy as they should. They share their data with everyone. They share their passwords with everyone. My daughter ...and we were talking before we started, we talked about our children. My daughter. I talked to her a couple of weeks ago because I couldn't log in to Apple TV and I thought, what? How did I forget my password? And I texted my daughter and I said, did you change the password? So children are... they change passwords. They share passwords. And I think it just complicates our effort to protect them.

[Arun]: Right. And you're absolutely right. On top of all of this. Most of my... I have two children under the age of 15. All of their data has already been compromised. They don't even know about. So by the time you're, you know, 10 or 12, your data is out on some database out there, whether you liked it or not, whether you willingly gave it or not. They've all got monitoring for every one of them because there was some dentist that was hacked. There was a pediatric dentistry that was hacked. Someone, somewhere lost their data already. They just don't even know what you were talking about, which is their relationship with privacy. The privacy contract is very different between what they live and what you and I, who evolved, with technology I call it. You know, we're like the old school, what we evolved with the Internet to the Internet. So our privacy contract, we're a little bit more suspicious of what we sign up for and they're not. You're absolutely right. And there's a third factor to this, right, which is where are they learning about cybersecurity? Where are they learning? And I have a great, you know, analogy of that, or rather, you know, a great parallel for how, you know, where they're learning. Well, look at the number of Stanleys that got soled during Christmas. Every middle schooler I know now, I have a child who plays lacrosse and that every person in that lacrosse team had a Stanley. This is like the hottest selling Christmas gift out there. People were fighting. Where are they learning about this? There is network TV as it existed doesn't exist anymore. Or shows for these things. Learning about this on social media, they're learning about it on TikTok. They're learning about it on technologies where, you know, privacy is being you know, they're losing their privacy as they learn about.

[Kevin]: Right, right, right. And it's a.

[Arun]: Address it. I And it's... there's a paradox...

[Kevin]: There's a paradox ...to their connection to technology is stronger than any generation. And their understanding and appreciation of privacy is weaker than any generation. And I think when it comes to parental and school district awareness, Arun, I don't think we fully understand that children are uniquely positioned to be victims. If you steal a child's Social Security number, you've got the keys to the kingdom for identity theft, fraud. And once that happens, I think a lot of our audience knows, once you've been the victim of identity theft or fraud, it can be very difficult to right the ship. Very difficult to explain yep, that wasn't me. That was a fraudster. Those transactions aren't mine.

[Arun]: Most adults have a hard time. Most adults have a hard time recovering their identity if it's once it stole. Now I've talking to teachers, parents all across the nation and children in K through 12. Yesterday, I spoke to some kids in high school. In high school. And every one of them knew at least four to five other people who had had multiple social engineering attacked attack attempts. What do I mean by an "attack attempt"? They received a direct message on Instagram from someone that was not a friend of theirs. All of them are aware of it. Some of them are like, yeah, I keep getting these messages. I don't know what they are. So it's happening. They're being targeted. How many of them have been victims? I know some statistics that are pretty staggering because you don't need a lot of victims here, because the victims are there. The stories when you hear them, you're like, wow, who's watching this? Yes, the numbers have gone up when it comes to young teens with generative AI, deep fakes would say those are.

[Kevin]: Easier to perpetrate....

[Arun]: And they're getting easier and easier to perpetrate harder and harder to discern. I work with some FBI groups out there in Washington, DC, where we're talking about, you know, people committing suicide because they thought that these images were real. Some of them are just, you know, falling victim to crimes and not knowing who to turn to. So we've got a problem that's brewing that no one really wants to talk about because this is one of those hard problems to solve. It's easier to blame systems, though, right? It's harder to get to the endpoint.

[Kevin]: I think that's right. And I think part of the... at least one of the problems as you're speaking and thinking, one of the problems is endemic to education itself. So as a lawyer, I know to go to the case books,

and the statute books, and maybe secondarily the treatises and the commentaries to find my sources of law. And I rely on those and I know them. By the same token, that if I'm on Google or Safari, or if I'm looking at a Wikipedia post, I should be suspicious of that. And that seems to be the opposite approach that young people take today. And of course, it's not their fault. You have a conversation with one of your teenager... or one of your children and they'll say, Dad, I just read this and I'll say, that's a little suspicious. Or as my daughter says, taught me, that's a little sus. So where did you read this? And she'll give me some source that is just utterly ridiculous. And I'll listen and I don't criticize her, but I say, you know, sweetheart, unless you're reading the New York Times, the Washington Post or the Wall Street Journal, you should probably be suspicious of anything you read on social media. So that's a huge issue for education, because we need to teach our children what are the viable, what are the valid sources of data, and what are the suspicious ones. I'm not sure we're doing that. We're letting kids... I see it in my show. Your kids, they're doing papers and you're sitting there saying, oh, well, how did you look this up? Thinking, I had World Book Encyclopedias. And they're going online and they're not discriminating between sources. So that's an issue, too I think.

[Arun]: It's a huge issue. And I think part of the you know, when you look at education, K–12 right now, right more schools now, my kids go out, one of them goes to a public school, one goes to a parochial school. Most of these schools across the nation give the kids Chromebooks. So we're starting to give them technology. But what do they do with these Chromebooks right? They create a white list and say, well, you can go here, you can go there, you can't access ChatGPT. We police, we don't teach you. We don't tell them why. We're just like, hey, don't use write up works because you never explained why you never taught them. You just restricted it. It's the "wet paint" problem, right? Right. No doubt people want to touch it. Why? Because you just made this more important than it was. Instead, if we actually took these technologies and taught them and this is what the Cyber Hygiene Academy hopes to do, we want to enforce we want to do what the school system is, not do it. We want to create cyber hygiene in our children. We want to instill cyber...and cyber hygiene is, you know, there are three Rs that we want to do, right. So what are these three Rs? We want to teach them to respond, to react, to recover. Right. How do you respond to an incoming attack or a call that's coming through? How do you resist it? Right. And if you do it, how do you recover? And when you do these 3 Rs, you get what is called is resilience. Right. And this goes across a spectrum of things that you need to do—everything from what you're talking about: credibility of sources. How do you use social media, what we call social media hygiene, email hygiene, messaging hygiene.

[Kevin]: Mm hmm.

[Arun]: How do you create better password authentication hygiene? And it's not just, hey, you know, create a new password. It's how do you craft these passwords?

[Kevin]: Yes.

[Arun]: How often do you need to do it. How do you how do you store them? How do you keep them in a manner in which everybody and how do you not shared with everybody around you like all your friends knowing a password? It's not a password anymore.

[Kevin]: Right. You have no protection. That's all good, Arun. And I think you're right. I remember when I was a kid, I was told "because I said so," affectionately, but firmly. And today kids want an explanation. So how about something like, "Well, the foundation of a free society is the ability to discuss and debate and decide. And if we can't agree on reliable sources of information and we can't secure our communications at the most basic level so that we know who we are talking to, who we're communicating with, we don't have a free society."

[Arun]: We don't. And we are creating a generation of children who are going to be in the workforce. And we're hoping that when they get to the workforce, they are going to become resilient. The problem is when your foundations are weak, the society that you build on those foundation continues to be weak. You know, we as a society are going back to where we were. We have dealt with problems such as this. Right. I mean, if you... and

you and I are very similar in age, you know, in the old school, you know, I think of a parallel of sex education. Right. In the seventies and eighties, you know, sex education, depending on the school you went to, you know, you would have a priest come in and talk, a doctor come in and talk, and then the school principal will come in and talk. And what would they say? Right. The priest would come and say, don't do it. The doctor would come and say what not to do. Right. And then the principal would come and say, where not to do it. No one would explain anything about the how, the why, the rationale behind it.

[Kevin]: Right.

[Arun]: That's the problem. And what changed that was the 1980s, the AIDS epidemic. And what we had to deal with it after... what we had to have hard conversations. And what if you look at HIV and AIDS and how we combated it as a society, which became ballooned into what the process was all across the world is we changed orientation, we changed how young people orient to sex. We didn't...We explained the rationale, but orientation to sex changed. It wasn't just the commercials that changed it. It was the orientation. Today, whenever you have people in a first encounter situation they orient themselves saying, well, you know, I don't know this person, I gotta have safe sex...

[Kevin]: There's a heightened awareness that do.

[Arun]: See a starting point be changed. How generations orient to sex. We have dealt with this and we've done it very well. And we need to do a very similar thing with cybersecurity, with cyber hygiene, with cyber resilience. We have to change orientation. We got to begin with Y and that involves explaining what's wrong when you go to sources that are readily and easily accessible.

[Kevin]: Right.

[Arun]: What happens when you just go to Wikipedia? How easy is it to create a Wikipedia page and add entries to it? I don't know. Right now we have exactly. We have to change that orientation. That's more than a slogan. It's demonstrating what could happen. Likewise, we need to demonstrate to our kids what happens when you post an image online. How much metadata can I extract from it? How easy it is for someone to know where you are when you took that picture, how much of a threat is it to your personal self? So we talk of, you know, psychological hygiene, right? Personal hygiene and privacy. We talk about these three things, which is your sense of where you are, your location, your geography, all of these matter if there's a bad guy out there and remember these, you know, hackers and predators can be anywhere in the world.

[Kevin]: Yeah.

[Arun]: So this becomes very you.

[Kevin]: No, it's critical. And I think that leads us neatly into how we fix it. So what are we going to do? What are the steps that we take? And I think that, you know, what the first item that you focus on in your Dark Reading piece, we touched a little on training students, but I want to come back to that with the first item you focus on, which may not be self-evident, and that is fixing teacher shortages. So it's not self-evident in the sense that we know we have teacher shortages that we need to fix. But the question becomes all right, how does that help us improve a generation of children's cyber hygiene?

[Arun]: Well, you know, the biggest problem here is, you know, we have... I looked at some statistics, about a 55% shortage, 45% shortage of teachers. And in a survey that was recently done, 55% of people did not want to be teachers three years down the road. It's not an attractive profession anymore. Right.

[Kevin]: What are we doing?

[Arun]: What are we doing to.

[Kevin]: What are we doing to make that profession unattractive.

[Arun]: The one of it is, of course, we're not paying them enough. Right. I mean, a teacher, after maybe decades of work, gets seniority, gets tenure, depending on the school system, makes as much as a mid-level cybersecurity expert. But then during their 50s, there are not technically there to teach kids about the technology, you know. Right. There are very few, you know, 60-year-olds who can teach what TikTok can do or even understand it or value it.

[Kevin]: It, or even 50-year-olds. So your.

[Arun]: You need young people to teach young people because they know periods of the technology they're dealing with. So if you want to teach cyber hygiene, we got to start with young people. We need fresh, young blood in the system, people who understand the children. You know, we don't want old people alone. We need to attract young talent. We also have to attract technically trained talent, which is even harder right now when I talk to school systems across the nation, the big question every administrator has is who's going to do this teaching? Because the incentive system is to teach existing material that takes the whole school day. There's no time. There's not enough time in the school day. Right. And the question is, who's going to do it? So many of them have a computer teacher who teaches basic technical skills. Is that person responsible or is it something that every teacher has to do? Which is how the ...New York State came up with a new set of mandates for cyber safety education. They said, well, it needs to be throughout the curriculum. Well, that's easy to say.

[Kevin]: It's very easy to say. Embed a culture of cybersecurity within every facet of your training program. And what you're saying is, okay, who are we going to get to do that? How are we going to...how are we going to convince teachers that are already... we already have a scarcity of teachers? How are we going to place this additional burden on an... existing teachers, presumably with no additional compensation? How are we going to train existing teachers to be able to do this? And then what are we going to do to try to attract new people into education who may have a closer connection to some of the problematic technologies? That's a lot of moving parts. And Arun, do you see it happening in school districts today?

[Arun]: I don't see it. To be absolutely honest, I don't see it happening. I just don't see it happening. I think this is too heavy a lift. There's you know, it just adds to the burden of the schools and the systems. And it's great if you're wanting to point a finger at the system.

[Kevin]: Right.

[Arun]: And that's not what I want to do. But I can tell you that that is not going to work. It's not blaming the system. I just think the system is not built for it. It's not equipped to go because we have not. We have to still teach basic knowledge. Cybersecurity comes on top of all of that. And so there's a question of where's the value in it? Do we see the value in it in our children now? Sure. What are what? How are the children learning them? Right. So I don't see it happening. I don't want to blame the system, but I don't think the system is built for it.

[Kevin]: Right. But your children are not going to learn good, effective cyber hygiene online or from their friends. They're going to learn at the most logical place they're going to learn it, is in school. And whether it is embedded within the curriculum, which I think makes the most sense to me or it's a kind of adjunct driver ed type course where we're going to bring in a third party service provider to provide that that type of education. It has to be done because we're going to raise a generation of irresponsible adults or... and adults who do not understand the risks.

[Arun]: Right. Or we're going to have to fix it down the road when they come to an organization to work, which is what we are doing right now. So right now, you have people coming into the workforce and then the employee is taught the first year. So you spend two months onboarding. And so if you want an upward cascade in skills, you want to train them right at the get go. It's no different than driving, right, using the driver's ed analogy. Right. We don't wait to teach our children to wear seatbelts before they start driving. We start right off the bat when they're kids. Yeah, we have to use the same principle. You start right off the bat and it probably has to be an external provider, which is why, you know, I said, hey, if no one's willing to do it, we'll do it.

[Kevin]: Right.

[Arun]: And there is no one willing to do it. I'll tell you why. Because school systems as it is are creaking when it comes to budgets. Nobody no organization in cybersecurity that I know and I work with, many of them is willing to take this on because there just isn't to use, you know, a capitalist view on it, there just isn't enough money in it.

[Kevin]: Right. Right. And yet it has to happen, you know.

[Arun]: You have to ask the question, which I've been asking parents all over the nation: where are your kids learning while they're learning from their friends who know less than them or just as much. They're learning from social media. And the bulk of the burden is to you and I as parents.

[Kevin]: Mm hmm.

[Arun]: Parents. It's a kitchen table conversation right now.

[Kevin]: Yeah.

[Arun]: That's where we're learning. Every parent sits down and says, hey, don't do this. Don't put your photos out there. Don't do this, don't do that. That's great. But it's not good enough. Right. Parents can't shoulder the responsibility. We need organizations out there that can do this for them, which is what we're trying to do. We're saying we'll be that organization that makes it interesting. It's not going to look like a classroom. We're not going to make this curriculum that, you know, kids don't care about. We're going to try to make this... I don't have the answers for it yet, but the goal is to come up with a program that will be interesting, that will be less of talking down to them. It'll not be like that priest and the doctor and the principal. It's going to be more like, how do we change our orientations towards all these different facets of cybersecurity? That includes things which you talk about, right? All the way from source credibility to email credibility. Right. Because the generation that we're... like you said, we have to create a generation that has a strong foundation.

[Kevin]: I think this is the most important recommendation you have. Training. Training. Training has to be built into our educational system. We're coming up on our time, though. There are a couple more I wanted to discuss with you, one of which very interesting, and that is reformation of credit monitoring for children. So I just settled a data breach class action yesterday. As part of that, one of the class benefits was additional credit monitoring—an initial phase of monitoring was provided after the notice of the data breach. We were going to extend that as part of the settlement. But you're talking about credit monitoring specifically for kids. Why do you think that's so important? And then let's talk a little bit about how it would work, because I don't think we have an infrastructure yet to make that happen.

[Arun]: Well, let's look at where this all started. Right. We had no breach notification laws.

[Kevin]: Mm hmm.

[Arun]: And then, you know, a lot of us advocated for it, and then we followed the California model. And breach notification is now standard. But what do you get right when a notification happens as part of a class, the consumer gets credit monitoring. How many consumers out there actually utilize it? We don't have the data.

[Kevin]: We the data we have from the credit, from the claims administrators that we retain. It's I'll be very conservative. It's less than 5% and in some cases less than 2%. I mean, it's just one very, very small.

[Arun]: Very. So, people are not taking it seriously. Right. Number two, these credit agencies, what do they eventually protect? They protect your financial credit.

[Kevin]: Mm hmm.

[Arun]: This isn't built for identity protection in the way people think it is. Right. So they're not going to protect your photographs that are out there, your reputation that may be marred. I mean, that's what lawsuits are for. But this is basically just protecting your Social Security number and their financial history. So it's a very minimal protection. It's better than nothing. Regardless, most people don't use it. When it comes to kids, it's even worse. Many of us, many of our kids, both my kids do they already have so-called credit monitoring because they're already victims of a breach that they don't even know about. They don't even understand what the ramifications of these are. As a parent you try to lock their credit, which is essentially one thing which this does. It's not easy to lock your credit. My recommendation is... we have three agencies right now which are for-profit companies. What they need to do is lock everybody's credit as a default. That's first. Especially kids, right? There's no reason and it needs to be kept open for me as a parent to go out and lock it. It should be locked by default and it should be monitored for life universally, not only after someone has a breach somewhere because no one's going to sign up for it. This point, though.

[Kevin]: Statistically.

[Arun]: We know that statistically and this is a generation of children who don't even understand what they're getting in, they don't even understand what that really means until their 18 and then and are they ready to get a credit card at 17 or 16 then? And that conversation happens around our kitchen table. That's not how the system needs to be we need to protect them under the default assumption that their credit is going to be breached or it's already been breached, that essentially protects more of us or most of us, especially kids who are out there, you know, in lower socio-economic rural areas, for instance, in lower socioeconomic urban areas who don't have the efficacy, don't understand what's going on. They don't have to suffer a breach in order to get protection. They should always be protected, as far as I'm concerned, up until 18 or even 21. Every child should have free. In fact, I think all of us I know these are for-profit companies and there's a price. And if you've ever tried and I do this right, all I've locked all our credits for the last two decades of our lives. But if you ever go online, the system has gotten better. So you go to Experian or what have you, and you try to remove your freeze, security freeze. You or I, we're technologically pretty savvy. This is not a seamless process.

[Kevin]: Right? No, it's not.

[Arun]: They're going to throw all these things. Are you saying, hey, would you want to sign up for this? It's no different than getting into a scam website and you don't know. Do you want to sign up? For now, they have a credit. You want to click here, you want to click there. And by the time and...

[Kevin]: I just want to unfreeze my credit.

[Arun]: Yes. And just, you know, out of the three agencies, one of them will not work online. You'll have a call to them. So it's a constant moving target. This is not consumer friendly. It was never built for you and I to use... this is built for credit card companies to know your financial to reduce their risk of giving you a loan.

[Kevin]: Right.

[Arun]: That system was not built for what it's being used for. So we need to reform the system and say, okay, what do we want an agency that protects more than just your credit? Perhaps what we want to do is expand the scope of it to say, reputation management. We'll tell you what stuff about you is online. We'll tell you. We'll monitor anything that's online and put a freeze on those would stop those things from showing up on search engines, for instance. That's a service that's actually there in other parts of the world. Right. So you go to Europe right now and you request as a Europe as a EU citizen, Google, Google remove the search term, they'll do it. In the United States. You don't have the same protections. So you should not forget laws are not the same. But maybe that's also part of what we need to talk about here because like you said, our kids are getting into this world with their privacy contract is very different from what you and I have, which means they're more than likely to have more stuff about them. Imagine, you know, I always talk about this to my children. I said, imagine you're running for office 25 years from now. What's out there about you today? That they're going to fish out... In those archives on social media, you never want to have something out there that you.

[Kevin]: No, no.

[Arun]: In that hard conversation you have with our children.

[Kevin]: Right. And I think I think that we come back to this as we close. I think that there's a perception that children care less about privacy, that this is a generational shift. And I don't ...I'm not sure that's the case. I think that when it comes to sharing passwords, that's one thing. But when you ask children about whether they want their personal communications with friends or family or photographs that are intended only for them or a very small group shared with other people, you're going to get the same answer that you get from every other generation, which is, no, we don't. And I think in the end, we're talking about cyber literacy for kids to some degree. And if we frame this issue in the right way, eventually for kids, but first for the educators and the legislators that need to make this happen, we have a chance to make it work. But somehow, either directly in the education system or through party service providers like the organization you founded, there needs to be an infusion of cyber literacy in our education system. I don't think there's any way around it. I don't think there's any other way to solve this problem.

[Arun]: That's right. And we need some systemic changes. We have to have systemic changes. But those things, as you know, happen over the long term. Reforming credit? Easier to talk about. Very hard to do reforming how we pay teachers, easier to talk about funding schools. We've been talking about it for generations now. Yes, there's one thing the private sector can do. We can inject that knowledge into the system faster than anybody else. And I think—and I have thought a lot about this as I founded my organization—I think the private sector has to do it. And the reason is that tech moves very fast, school curriculum move very slowly. It doesn't change much. Right. You can teach history. It takes a year for you. History doesn't change in that year. Tech has already evolved and we have to ChatGPT. Two years ago, we weren't talking ChatGPT right away. Right. We need some organization that can be that quick in saying hey, here are the new threats, here are the new skills, here are the new things out there. And that is something I think the private sector can do and can do very well. And they can pay and attract the kind of ...compensate the staff to get them to do it. We got it. But that's why if no one else is going to do it, let's do it. Because, you know, this is my contract with my kids. I have a 15-year-old and an eight-year-old, and it's my contract with my children. By the time they're done, I at least want to have one program that they can say, hey, you know, this taught me how to be cyber safe, how to be a resilient. If I can do that, I can save and protect those two kids my own. It's a very selfish motive, and I think I can do that. And if we can do that, we can protect every kid out there.

[Kevin]: Yeah, well, that is our charge. And that's very well said. Arun Vishwanath, thank you so much for joining us today on Cyber Sip and give us the name once more of the new organization that you're founding to try to make this education happen.

[Arun]: That's right. It's called the Cyber Hygiene Academy. And you can find us on Cyber Hygiene Academy dot com.

[Kevin]: We'll look for it there. All right, Arun, thank you so much. I really appreciate your joining us a second time. And I know you'll come back for another episode, where we will be talking about some other cutting-edge topic in the realm of cyber hygiene.

[Arun]: Absolutely. Thank you, Kevin, as always. It's a pleasure.

[Kevin]: Oh, my pleasure. Thank you. And thanks to all of you for joining us on this latest episode of Cyber Sip. We're back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.