NCF #CyberChats Podcast Episode 006 - May 11, 2023
00;00;00;01 - 00;00;18;03
BiaSciLab:
All computers-- you think binary, you think ones and zeros. In the end, it's all just math. So you have to have some understanding of math and how things work to be able to build with it. And it's also good to know how things work, to know how to break them, because you can easily find what the vulnerable points are.

00;00;22;27 - 00;00;52;13
Jen Langdon:
Hello and welcome to CyberChats, a podcast made by the National Cryptologic Foundation. I'm your host, Jen Langdon, and together we'll be demystifying the world of cybersecurity by talking with amazing cyber fanatics like you, as well as industry professionals.

In our final episode this season, you'll hear from a young person who is also a key individual in the cybersecurity community.

00;00;52;27 - 00;01;16;04
BiaSciLab is 16, a senior in high school, owner of her own nonprofit GirlsWhoHack, and developer of Secure Open Vote. You heard that right. She's not able to vote, but she has made a secure voting system. I could go on or we could dive right in.

How did you get to be in the cyber space? Tell us about your journey.

00;01;16;21 - 00;01;38;21
Bia:
Well, my dad has worked in cybersecurity and just in the tech field his whole life. So once I was old enough to read and write, basically, he stuck me into as much cyber and tech related things as he could. So I started programing with Scratch, which is just a block based programing language, which was really fun. So there is that and I've always been an extrovert.

00;01;38;27 - 00;02;01;05
So Dad told me that cybersecurity conferences where thing where you can go meet other people who work in the tech field and other kids my age who their parents brought along to. And I'm like, That sounds so fun. So I went to a B-sides conference. Besides, Delaware was my first, I believe. And when I was there, I met so many amazing people.

00;02;02;01 - 00;02;22;18
Even though most people in the tech field are introverted, they're still able to, like, answer any questions. I could walk up to someone on their computer and be like, What are you working on? And they'd explain it to me, Oh, that's really cool. Yeah. Yeah. I also did like one of my first talks there, which was actually a crypto talk, How to write Secret messages to your friends.

00;02;22;18 - 00;02;28;10
And it was, it was really fun. And since then I'm like, This is kind of what I want to do. This field is fun.

00;02;28;27 - 00;02;34;25
Jen:

What about secure open vote? Because I know that's a super big project that you have been a part of.

00;02;35;09 - 00;03;08;27
Bia:
So DEFCON is like the end all be all hacker conference, at least in the US it is the largest hacker conference, so 35,000 hackers each year in Las Vegas in August in the hottest, wettest weather ever they had back when I first started, they had the r00tz Asylum, which is like the kids track of DEFCON. After the 2017, maybe, at the r00tz Asylum, they held a mock election reporting system for us kids to try to hack and change the election results.

00;03;09;05 - 00;03;28;18
I think it was based on a system that they used in Iowa or something like that. And keep in mind at this point, I was like 11 and could barely type on a keyboard, let alone hack anything. But they gave us a little information packet. If you go on my website, you can also see like photos from that and you can see like a little pack in front of me.

00;03;28;22 - 00;03;54;16
It's me and a bunch of like 8 to 15 year olds hacking this thing. And we all have been under 15 minutes. And me being a kid, I was never interested in anything. Election related. Like there's so much misconception almost when it comes to voting that it's just like an adult thing. And I know kids should not necessarily be involved in politics because they can be more easily swayed, but they shouldn't at least know how our government system works, you know?

00;03;54;17 - 00;04;22;10
And I just didn't know anything about it. But once I saw I could hack it, I'm like, why is the system so flawed? So I talked to people at the voting village at DEFCON, and I met a bunch of people, watched a lot of documentaries and did a ton of research on all things elections. And around that point, Congresswoman Mikie Sherrill of New Jersey invited me to go to a congressional hearing on election security.

00;04;22;20 - 00;04;44;21
So I got to see the panel that was there and all the congressmen and woman talked to them about their concerns and questions when it comes to all things election related. And I'm like, I can build a better system than what we have now. I wanted something that was open source with a paper trail so that everything could be tracked in a physical way because a machine can be hacked, a piece of paper can't.

00;04;45;23 - 00;05;06;29
So that's when I started to secure open vote, my own end to end election system. I created the reporting system since that's the first thing I also hacked and I brought it to DEFCON and I brought it internationally to death camp. Not to be confused with def con told people, told the hackers, okay, try to hack it. Tell me how I can make the system better.

00;05;07;04 - 00;05;14;25
Tell me what's wrong with it. People tried to hack it. So far it hasn't been hacked. That doesn't mean it's unhackable, but it means it's pretty secure so far.

00;05;15;08 - 00;05;23;23
Jen:

So why is that so important? Like, how do you envision secure, open vote being used? Do you or do you envision it being used widely like.

00;05;24;01 - 00;05;34;15
Bia:
I'd hope so. I hope to get it, yes, because now, even though there is a bunch of different voting machines and things, there's two big companies that overrun the entire election and they're actually in--

00;05;34;24 - 00;05;39;21
Jen:
It's a consolidation of all of those resources. Yeah, they're the company.

00;05;39;21 - 00;05;57;11
Bia:
Yeah. So it's really just one big company that does it. And they since it's they have like no real competition, they don't really care about updating thing. I mean the things I mean they reuse the same machines they've used for years and years that have been hacked. And like at DEFCON they have the voting machine hacking village. All of their machines are brought there.

00;05;57;28 - 00;06;24;24
They hacked all the machines in under 90 minutes. So obviously they're easily breakable. Of course, there's a big discussion like were the elections hacked? Did this person win actually, or did it was it because of this? And I realize that if you have a paper readable trail that puts everything into like physical proof and then you hand count the votes, there's no real way to fight against that.

00;06;24;24 - 00;06;47;23
Even if the actual votes were hacked. So that's why I wanted my system to be completely open source, but still secure. I wanted something with like no back doors that we go and change the system within the middle of election. I just want something open so that people can understand how it works and understand why it's so secure and good.

00;06;47;23 - 00;06;57;17
Because now, like even when I talk to my friends who are also teenagers, they're like, I don't know if I ever want to vote when I'm an adult. If it's the system's already flawed, what's the point of voting?

00;06;57;17 - 00;07;21;16
Jen:
That’s a huge point. Yeah. Like with out the knowledge that it is secure, then that puts everything else in jeopardy. So tell me like, what do you need to know to create something like this? Is it math? Like, do I need to know about all of that to get myself on your level in terms of like creating a secure voting system or creating something that is secure? Do you know what I mean?

00;07;21;17 - 00;07;42;06
Bia:
So when it comes to anything cybersecurity or anything security related, you'll hear the term red team and blue team being used a lot and even purple team. So the whole definition behind that is Red team

is the hackers. The attackers, not the bad guys. Not necessarily. At least it's people who break into things.

00;07;42;11 - 00;07;58;23
And then the blue team are the people who build the things and secure the things. So it depends kind of what field you want to work in. I'm personally I'm more of a red team kind of girl. I like to break into things, try to wiggle my way and see what parts are not secure and how I can use those to my advantage.

00;07;58;23 - 00;08;24;28
Whether that be a physical machine that I can compromise, whether that be like a server I can get into or even a person, I can fish and then get in that way. But if you're someone who's more of a blue team person, which I kind of had to be to create my system, then you need to know programing and those kind of things and programing and machines at the base of it are all math related.

00;08;25;07 - 00;08;50;22
Like Ada Lovelace, for anyone who doesn't know, is an amazing mathematician and from back in Victorian times who created the first computer ever, which was a math machine. So all computers at the end of it like you think binary, you think ones and zeros. In the end it's all just math. So you have to have some understanding of math and how things work to be able to build with it.

00;08;51;05 - 00;09;05;02
And it's also good to know how things work, to know how to break them, because you can easily find what the vulnerable points are. And then of course, there's the purple team, which is worrying about defending and attacking.

00;09;05;24 - 00;09;17;20
Jen:
But this whole cryptology and cryptologic knowledge, like that's critical to part of securing the project. Right. And securing the vote. Is that so? Yes.

00;09;18;21 - 00;09;39;13
Bia:
When it comes to codes and things, you always hear the word thrown around the whole encrypted thing. Yeah. Like your messages are encrypted, your emails and encrypted send one can get into it. It's it does work that way. A machine to be able to read a message would need the key to decipher the message that goes again with Wireshark and like packet capturing.

00;09;39;13 - 00;09;56;02
Like I mentioned earlier, because if you send a message to someone and let's say I want to send you a super secret message, I would definitely have like an encrypted email or something so I could send you the message. And if anyone tries to capture it in the middle using a packet capturing thing, they'd see, Oh, this message is encrypted.

00;09;56;02 - 00;10;13;14
I'd need the key. So it'd be even harder to try to crack that code. There's also you hear the term secure messaging. So like messaging apps like Signal, which should be used, which has encryption so that if anyone tries to get your messages, they can't without the key.

00;10;17;00 - 00;10;39;19
Jen:
Here's your challenge note for this week here. Develop this week's challenge. And if you're one of the first to crack it, you can get yourself some free swag from her on top of the prizes that will be handing out at the end of the season for individual and team participation. Be sure to submit this last challenge to increase your chances of winning some sweet stuff.

00;10;40;01 - 00;11;03;18
The Episode six challenge is live from May 11th to the 24th. This challenge doesn't require any fancy equipment, just some pencil and paper. Okay, I lied. You might need the internet to search for information or to check our Instagram for clues. It may be very involved challenge for you, especially if this is your first crypto puzzle. Keep working it.

00;11;03;19 - 00;11;25;19
You got it. Good luck. If you sign up to our mailing list on our website, you'll get notifications of when the challenge leaderboard is updated. And when we come back for season two. Oh, that's right. We already have some amazing guests lined up for you and new topics to explore. What are you waiting for? Go on our website and sign up.

00;11;25;19 - 00;11;41;18
And while you're at it, check out the last challenge of season one. Find it at cryptologicfoundation.org/ podcast.

Tell us about what inspired you to start Girls Who Hack.

00;11;42;00 - 00;12;08;16
Bia:
So when I was younger and I went to all these conferences, I did notice women in cybersecurity and obviously there's way more women now than were before. But the proportion of like women and minorities rather than old white men, to put it simply, is like still pretty unbalanced. And I'd like to have more of a like even playing field, if that makes sense.

00;12;08;29 - 00;12;33;20
So there are women in cyber, but I didn't really notice any girls in cybersecurity. And there's I went to a conference and just like kind of like a girl power sort of conference thing and Reshma Saujani, she runs Girls Who Code not to be confused with girls who hack, which teaches girls how to program in code. And you should definitely go check her out too.

00;12;33;21 - 00;13;00;16
She has a book called Brave Not Perfect, one of my favorite books. I highly recommend that too. And she sort of inspired me to start Girls to hack that in the fact that there's not enough like girl support. Because even if like, I don't know if you've ever experienced this too, but if you go to a conference or anything cyber related, it's kind of difficult being the only woman in the room without like support or there's only like three girls and then 20 or 30 guys, you know.

00;13;00;27 - 00;13;34;15

So I wanted to create a space that was like aimed specifically at girls so that we can help and support each other and learn together. So I've done online in-person classes with girls who have taught like soldering classes, very intro, basic classes. So if you can use a computer and a mouse and you can do it because all of these basic classes like air quotes here online, save their intro classes, but then they say words like servers and database, but they never explain what those are.

00;13;34;16 - 00;13;53;18
That's not an intro class. Yeah, like you need some foundation level. So that's where my classes come in and that's sort of why and how I started Girls to Hack. And my future plan with this is to get the show more on the road because usually I stay more on the East Coast because that's where I live. But I'd like to take it over the US and definitely internationally someday.

00;13;54;17 - 00;14;32;26
Jen:
Yeah, I think it's really insightful that you recognize that vocabulary is a barrier for some girls to be able to enter and participate in some of those classes, you know, like understanding all these different pieces. Those basic things are so important to reaching the next level for girls. So I kind of want to talk about something similar, like when you Google hackers, usually what shows up are and I literally did this before the show this morning, white males in hoodies is like for 50 images.

00;14;33;00 - 00;14;54;18
So it's not even just like the first two or three. It's like the whole page or two pages. All black clothing is the next thing and there might be energy drinks or something, you know, like there's a keyboard, there's computer, and then that's it. Why is it important that we break that stereotype of what a hacker is? And how are you doing that?

00;14;55;17 - 00;15;16;05
Bia:
Like you said, it's always like the white male with the hoodies and stuff. Yeah. And like even portrayed in media, like movies and things that like hacking and then they say just random words like, oh, and I'm into the cryptologic called database of the NPC net and I'm about to pacify the wall and then they're just typing away and the ones and zeros coming down on the screen.

00;15;16;11 - 00;15;44;14
And of course that looks great visually, like on a movie standpoint, but it's, it's not real life. But that mysskin ception comes and then people think that hackers are bad guys and some hackers are. There's good hackers and bad hackers in the world. I want to like sort of separate that now because the bad hackers are obviously the ones you care about, the ones who create like the WannaCry virus, which was back in 2013 that took down medical systems and things.

00;15;44;21 - 00;16;03;24
And then if you look on the news, you're like, Oh, the pipeline was breached. I know that was like a big thing. A pipeline? Yep. And just all of those things and you hear hacker equals bad. But really hackers are good guys too. Usually they go under the name of like cybersecurity something. So they don't say like my job title is hacker.

00;16;03;24 - 00;16;28;16

But there's penetration testers who get paid to hack. So like if a company says we want you to come hack into our system so we know what's wrong with it and how to make it better. So if a real hacker tries to attack us, we'll be better prepared. So if you're a penetration tester, which is usually a red team person, then you can go in hackers and some say, Hey, this is a bad part of your system.

00;16;28;16 - 00;16;51;18
You need to better encrypt it or you need to use this. This needs to be updated. So it's good to break the stereotype because it gets more people interested in cybersecurity. Because when you hear cybersecurity, you're like, Oh, that's a bad hard to get into a field. And I'm not going to say it's an easy field, but it's such a widespread field with so many different people and so many different career choices.

00;16;51;23 - 00;17;03;17
It's kind of like music, you know, how there's endless genres of music and list singers, endless songs. It's kind of like that with cyber security because you have all the blue team people, the red team people, purple team people, people that build stuff and break stuff.

00;17;03;20 - 00;17;27;00
Jen:
I love this analogy, because you made it seem like a chorus, right? Like a bunch of people are playing together. Like people understand when you go and you study music or when you go do music, like people understand. Musical artists work really hard at doing all that stuff. It takes a long time. And with cyber, it doesn't happen overnight either.

00;17;27;10 - 00;17;51;22
It takes lots of time. You have to be persistent, especially if you're if you're hacking or practicing anything. You're doing cryptology. Like that's not going to happen. It looks confusing, right? Like, it's going to take time to sit with it and learn it. And I think that really like for me and hopefully a lot of people like kind of grounds the idea of like what cybersecurity is.

00;17;55;01 - 00;18;17;13
You may or may not be on Bia's level, but how can we know how to keep our information secure? You can get started by joining us for Cyber Saturday on June 10th, 2023, at the Dream Port facility in Columbia, Maryland. Current and rising fifth through ninth graders can learn about cyber data care and online safety through fun hands on exercises.

00;18;17;23 - 00;18;35;09
Plus, adult chaperons can join in the fun, too, by trying out the National Cryptologic Foundation's escape room. It's a perfect way to kick off summer. Mark your calendars now and stay tuned for registration details on our website at WW Cryptology Foundation dot org.

00;18;39;15 - 00;18;48;25
Is there anything you'd share with our listeners about taking care of their own data? What would be the best way to protect themselves from hackers?

00;18;49;13 - 00;19;13;11
Bia:

Number one, definitely change a lot of your passwords if they're not like this, but there's a big misconception when it comes to passwords. It's like you have to have the most complicated password ever, which is kind of. Yes, But it's more important to have a passphrase. The longer the password, the harder it is to crack because a password cracker goes through every single option.

00;19;13;16 - 00;19;34;12
It's not just a guy going on your computer and like, okay, let's put in their birthdate first, which of course some hackers do that, but usually they just put this tool on. So it doesn't matter if you think it's complicated, if it's long, it's going to take longer to crack. So like a decently long password that's like 11 characters, long would take years to crack into it, and they'd probably give up after the first day, you know?

00;19;34;19 - 00;19;59;25
Yeah. So having a passphrase related to something and this used to be one of my old passwords, I don't use it anymore, and this is not exactly what it was. I had like a YMCA account or something like that. And I had I used to take swimming lessons at YMCA. I can still barely swim. But, you know, I had a blue unicorn bathing suit, so my password for that was like blue unicorn be a swim, but with different characters change.

00;19;59;25 - 00;20;22;01
So like some capitals, the lowercase and stuff, but I could remember what it was because that's what the countless about. Using a password manager is also important to another thing. There's an app called Signal. It's completely free. It's open source and it's encrypted messaging that's back and forth. They don't store any of your messages. So even it's like, hopefully no one does.

00;20;22;01 - 00;20;42;13
But if you've committed a crime and police are like, I'm going to go check your phone records, like your messages with someone else, they literally can't because Signal saves none of them. They just completely disappear from the trace of the earth, which real messages get stored. Don't click on random links and emails. Update constantly. If something says update, don't just click remind me later.

00;20;42;13 - 00;21;03;28
It’s not going to take that long to update unless you have a Windows machine, but it's better to be safe than sorry. Multi-factor authentication. Usually Gmail will be like set up a multifactor authentication do that. There's been people who tried to break into my account. Thankfully, Multifactor saved me there. And do your research and share what you learned.

00;21;04;10 - 00;21;21;02
You know, especially with like the older generation, the young, younger generation, like the iPad cocomelon kids all the way to your parental parents, you just you got to teach them what's wrong, what's bad information, You know, just spread what you learned.

00;21;23;00 - 00;21;41;29
Jen:
That's our show. Thanks so much for being a part of our community. We can't wait to see how you do with this week's episode challenge. Go to the CyberChats podcast page on our website at www.cryptologicfoundation.org to find this week's challenge, submit a question and join our focus group to help improve the podcast.

00;21;43;01 - 00;21;55;13
You can watch more of this podcast on YouTube. Be sure to like and subscribe to hear more and check out the show notes for more details and links. This podcast is made possible by the Chilton Foundation.