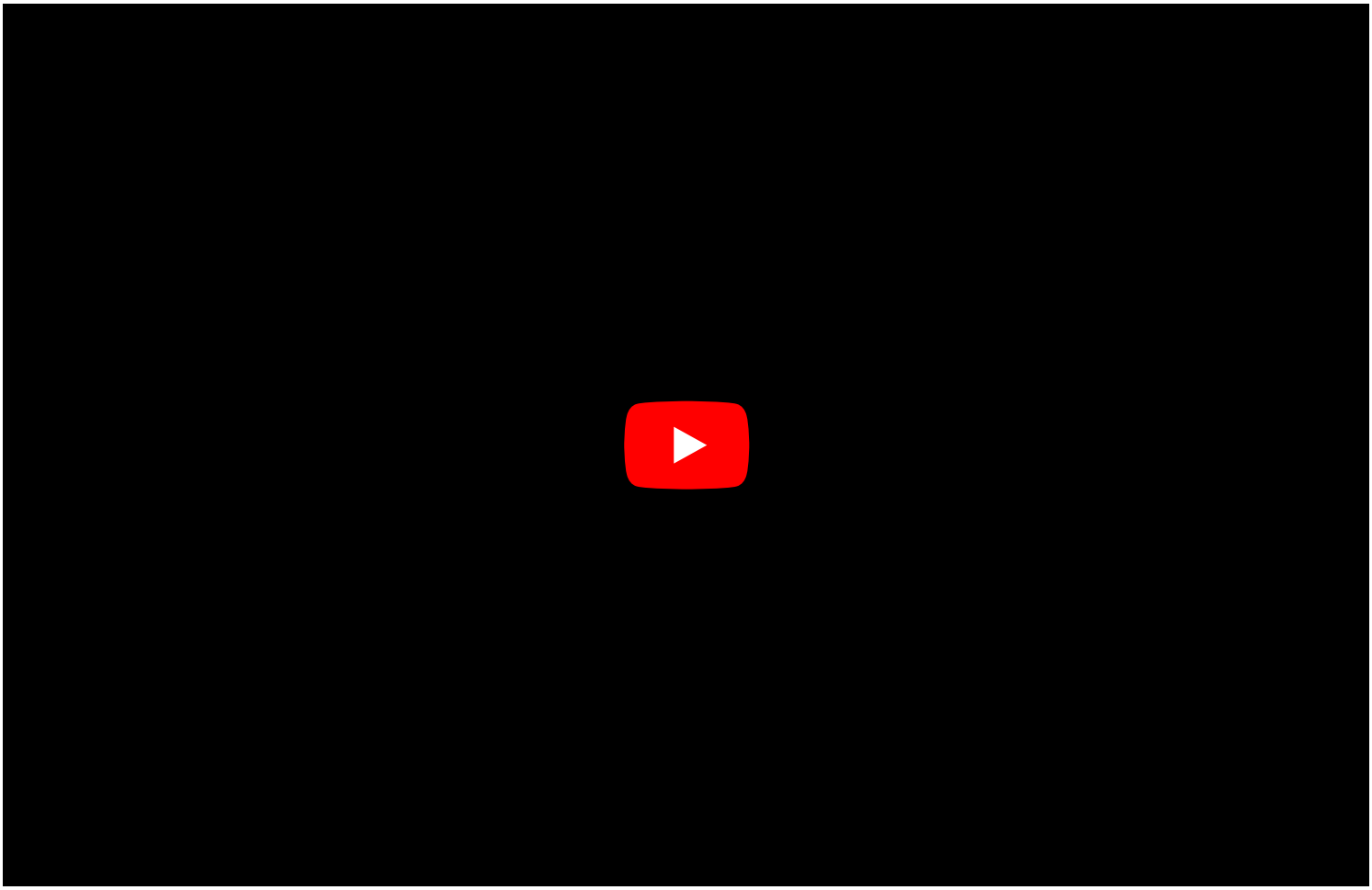
CARLTON FIELDS

S1:E4 - Raiding Your Vault: Cybersecurity in Gaming

March 26, 2019



Steve and Nick discuss cybersecurity incidents impacting the video game industry, from brute-force attacks to swatting. They also interview professional streamer Ben Bowman (AKA Professor Broman), and review potential legal recourse for those who have suffered a gaming-related cyber incident.

Transcript:

Nick: Hi and welcome to the LAN Party Lawyers podcast where we tackle issues at the intersection of gaming, law and business. I'm your co-host, Nick Brown.

Steve: And I'm Steve Blickensderfer.

Nick: And today we're going to be talking to you about cybersecurity issues facing video gamers in the esports industry. But before we get going, we have to remind you real quick that nothing we say here is legal advice.

Steve: So today, we're going to focus about cybersecurity issues facing video gamers. I am excited, very excited to have with us a professional gamer, content creator, all around great guy, "Professor Broman," Ben Bowman with us here today to discuss some of these issues. Ben, which we'll get to in a little bit, has had some firsthand experience with cybersecurity issues in gaming and how it can impact competition in the gaming space.

So to give a quick roadmap of where we're going, we're going to talk and lay the groundwork for cybersecurity in gaming, what that looks like; then we're going to, you know, that will involve talking about some recent hacks involving top games; how criminals use stolen funds to launder money, things like that. In the middle of all that, we're going to talk to Ben about some of his experiences and brainstorm some ideas, what are some of the legal recourses that are available and what are the gray areas where maybe there may not be recourses available and where maybe we should be thinking about, you know, shoring that up. So, without further ado, Nick, why don't you tell us what we mean when we say cyber security in gaming.

Nick: Sure so cyber security issues generally involve bad actors like hackers using computers or other internet-connected devices as cyber weapons to exploit code and security flaws in games or people that just aren't paying enough attention to gain access to another computer or system. And once they're in, they can do all sorts of nefarious things in the gaming space, like, you know, just from the bottom level, gaining a competitive advantage in a game but all the way up to causing a disruption in competition or breach systems to in fact scrap data and other info to find way to make or launder money.

Steve: So I may know this, but some others may not, but what is the difference between cybersecurity and data privacy?

Nick: Sure, so they're related but distinct concepts that are often thrown around together. Data privacy usually refers to the laws and regulations that revolve around collecting and using data, whereas cybersecurity issues usually involve a bad actor trying to do sneaky stuff to get your data and ultimately your money. We actually have another LAN Party Lawyers podcast that's dedicated to the data privacy issues that you should check out.

Steve: Right so we're strictly here talking about the cybersecurity aspect as it relates to gaming. So, Nick, why don't you give me some examples of cyberattacks and the various forms that they take?

Nick: Sure. So there are four main examples. The first one is the classic [one] that pretty much everybody knows about, these are viruses or other malicious code sometimes referred to as malware. In this example, hackers can introduce viruses and other malware to trick computer users to open infected programs, and once those programs are open the virus or the malware can steal data, it can lock up your computer, it can do all sorts of nasty stuff. PC gamers in particular are susceptible here because there's a lot more opportunity to download third-party programs that can augment ones gaming experience, that you don't know where they came from, or you don't know what people have done to them.

Steve: That's right, sometimes as a gamer you don't even have a choice but to click on that suspicious link. Another example is DDOS attacks or DOS attacks, that stands for the distributed denial-of-service or just denial-of-service, depending on how the attack is set up. But essentially the gist of it is there is one end that's sending a flood of information or packets of data to target the victim, and the idea would be either to drop that computer from having access or connection to the internet, or to overload a program or system to cause failure - whether physical failure or just software failure.

Nick: So it's just so much that the computer can't take it and it ends up ruining other processes too?

Steve: That's right, that's right. Another example of cybersecurity, cyber-attacks is social engineering attacks, sometimes commonly known as phishing attacks.

Nick: That's phishing with a "p-h."

Steve: With a "p-h," exactly. That consists of using low tech or non-technical approaches to persuade people to compromise security procedures and disclose sensitive information. So a recent example of that involved Fortnite, where accounts were hacked due to an exploit in the way subdomains authenticated logins. To fall victim to this attack was actually very simple: all a player needed to do was click on a link. It was a very carefully crafted phishing link...

Nick: Like a Trojan horse.

Steve: ...well that that introduced that, exactly, it was designed to look like it was coming from Epic Games. And then once clicked, the hackers were able to steal the user access tokens and perform an account take over. And once inside, the hacker controls the account, can purchase in-game items using v-bucks, or whatever the currency is, and even poses as players online talking to other gamers.

To increase the likelihood that someone is going to click on this link, as you can imagine [the hacker] would entice them saying click this link for 25% off v-bucks or whatever.

Nick: Which is especially scary when you think about the fact that Fortnite is a really popular game amongst kids and kids are probably more likely to be susceptible of that sort of thing than adults.

Steve: Terrifying, exactly. So once clicked, there's really no need for the user to do anything further. The authentication token was then immediately captured by the hacker. But fortunately in this instance Epic fixed the problem and solved that issue, but that is one example that does exist.

Nick: And the fourth example that we have is classic data breaches or theft. This is where people hack in either brute-force attacks or otherwise to get to the data of another. The goal is to commit fraud or otherwise obtain their data that is private and that they don't want you to have. One recent example of this was in Fortnite, there were some reports of criminals that actually created accounts and then used stolen credit cards to purchase in-game items - no doubt, using credit card data that was obtained through other hacks. And then once they got in, they made their account, they bought all of the stuff on the account and pumped it up, then they would turn around and sell it on a third-party site, like an auction site or something like that for a fraction of the cost, and thereby laundering the money in the process.

Steve: So, Nick, why is this a big deal for video games and the industry as a whole?

Nick: Well, crime and fraud is bad anywhere, but as the video game and esports industry continues to explode in the popularity that we've seen over the past few years, bad actors are going to be increasingly attracted to it and setting their sights to try to figure out new ways to exploit and take advantage of the people in this industry. It's particularly true given the fact that we're seeing a lot more money in the industry now with esports and esports competitions getting more popular and generating more advertising, with more micro-transactions in games, and as more credit card and bank information find their way onto game servers - the risk is going to go up, and up, and up. And as more money is on the line for these games, there's also going to be a greater risk of cybersecurity issues, it's just going to be a giant target that attracts these types of people.

Steve: That's right, so as we think about this, the next question would be who are the targets? So as you could tell from the examples that we gave, some of the targets would be those games at the very top where most of the gamers are playing and where most of the money is.

Nick: Your Fortnites, your DOTAs...

Steve: Exactly.

Nick: ...all the big battle royales that are out now.

Steve: In researching this issue, I came across an interesting stat. At the end of 2018, into early 2019, the top 50 Fortnite items that were listed on a very popular online auction brought in about $250,000 according to a report. So this obviously creates an incentive for hackers engaging in cyber-crimes to get a quick buck.

And another potential target would be esporting events. As you can imagine there's a desire to gain a competitive edge whether through a cyber-attack or otherwise, and that is definitely going to be an increasingly popular target as more money gets pumped into these esporting events.

Nick: Not to mention, everyday gamers, right? People that just want to play games in the privacy of their home, either online or on single player games, particularly the ones that end up following or having popular streams that engage with the public. And as it turns out, we actually have one of those with us today.

Steven: That's right, we have Ben Bowman with us, a professional gamer, broadcaster, fundraiser, hellraiser and all-around good guy with us on the podcast, Ben, welcome to the LAN Party Lawyers podcast.

Ben: Thanks for having me.

Steve: So I consider you to be like the Frasier of the gaming industry, giving great advice on your stream, "Ask Broman," that helps content creators and broadcasters starting out. But, I don't want to peg you as Frasier if you want to Niles.

Ben: No, Frasier's fine.

Steve: Okay.

Ben: My wife would be really, really happy with that comparison as well.

Nick: Are you listening, Ben?

Steve: So I understand that you actually started out with an interest in cybersecurity, is that true?

Ben: Yeah, so one of the last things I was studying before I ended up sort of falling into streaming fulltime, it was just something I originally did as a hobby was cybersecurity. So I was starting to get my certs and things like that. I learned enough to make me super tin-foil-hat-on-my-head paranoid about a lot of things...

Steve: Yeah.

Ben: ...but not enough to know everything to do about it, so pretty interesting situation, but yeah. So I had a passing interest in it much before I got into streaming fulltime, and it's actually served me really well since I've started because as gaming has become more popular there are always people who are looking to make things hard for you as a broadcaster, or Youtuber, or anyone online who might end up being a target.

Steve: So taking that experience and general interest in the area of cybersecurity, I would consider you to be above average on the education scale with respect to looking out for things and practicing cyber hygiene, have you ever...

Ben: Yeah.

Steve: ...experienced a cyberattack yourself?

Ben: Yeah, I have a few times. A game that people, if you watch me on Twitch, I'm "ProfessorBroman," one of the games that I'm known for is Destiny.

Steve: Mm-hmm.

Ben: Destiny has a pretty severe security bug that's been present due to the way they manage their networking...

Steve: Wow.

Ben: ...which is peer-to-peer that leaks your IP. So a big problem that they're dealing with right now is anybody who's in competitive situations in the game will have someone on the other side of their game pull their IP as they're match-making into whether it's a PvP match, or in my case it was a little bit worse, and use whatever they've got around their house or a rented server or whatever they might be using. It doesn't take that much to knock off a residential line and DOS or DDOS your connection.

My worst experience with it was during a "raid race." So if you're not familiar with Destiny, it has big capstone pieces of content called "raids." Every time one comes out there's a race for worlds first, it is the only time that race will ever happen, it's like the Olympics if there was only going to be one person ever who was the fastest person alive.

Nick: And it's individuals, it's not on teams?

Ben: It's a team-based thing, so every raid team has about six people in it, that's the minimum requirement. So during the most recent raid race for Destiny, myself and the rest of my team were knocked offline systematically during the race to prevent us from competing in it essentially.

Nick: Oh, no.

Steve: Wow.

Ben: And while there's not really a cash prize for this, there's a lot of rapport or status that comes with it.

Nick: Bragging rights are worth something.

Ben: Yeah, my teams gotten a world first before for another raid in Destiny, and we're in The Guinness Book of World Records for that.

Steve: Wow.

Nick: So do you think that's why they targeted you?

Ben: I think that there are a few reasons why we were targeted. One, we're highly visible. And our team got targeted and so did a couple other teams that traditionally are in the running to get world first. So I think people just wanted to throw a monkey wrench into the whole thing, which is really frustrating because you have this experience that you're trying to share with everyone - that's the whole point of broadcasting. And to have it sort of corrupted like that it's not just ruining one person's experience, we had 60,000 or 70,000 people watching across all of our streams during this. So it's like ruining an entire NFL game for everybody.

Steve: What did you do as a result? Like without getting into any specifics if you talked to any lawyers or anything.

Ben: Well, I have two connections in my house, I have a residential connection that I use for all my gaming stuff. And then I have an enterprise connection for my stream that's really robust - it's got six fallbacks, it's the same stuff they'll put in hospitals, so it's enterprise-level connection. It took them a few months to install. But I did that specifically as a security measure because this is my livelihood. And along with residential internet being dodgy sometimes if a person we're to grab this IP and even use a rented server to try and take down my connection, they might be able to do it for a second but the moment they did that I would get a call on my phone, there would be a tech heading out to the node by my house, and they would be ready to switch my IP and put me on a new connection on new hardware with new MAC addresses and all that other stuff.

That's an expensive investment for me, it's not the cheapest internet in the world. But that's the lengths to which I've gone to protect myself on my streaming side. For the residential connection, I just had to wait for them to stop. To finish the raid race, I tethered my WIFI from my phone to my gaming computer and then finished it over WIFI. Yeah, that's how we handled it, me and one other person had to do that, and I think someone else might have gone to another person's house, but it was very frustrating.

Nick: Whatever sacrifices you have to make to get that world first, right?

Ben: Yeah, we still finished in the top ten despite all the issues.

Steve: Nice.

Ben: Yeah, it was great, but you know it really stinks to know you had it, but there was this third party actor who really ruined everything for everyone, not just our team.

Steve: So what would you have done differently if anything? I don't know if you could have done anything.

Ben: So like I said, there's a specific, well there's one thing we could have done differently, but it's primarily out of my hands. So the one thing I could have done differently is not have, we could have just not had our party open.

Steve: Mm-hmm.

Ben: But because we're all broadcasters we default run our party on because we're playing with viewers all the time and it makes it easier for them to join us, it also unfortunately makes it easier for people to do this.

Steve: Yeah.

Ben: This is the first time in five years somebody used this particular method, somebody joined our party right before the race started and then we kicked them and that's how they got our IPs. So technically that's a vulnerability, a choice that we made for entertainment values that made us slightly more vulnerable, but going further down the pipe on that, the way that Destiny's server structure is set up - because it is peer-to-peer and they have these synthetic instances and things like that, there's all this IP handshake sharing and stuff - and it's been like that since Destiny 1 came out, and this has been a primary complaint of the community for a long time: if the game was on dedicated servers, this sort of behavior wouldn't be possible because you wouldn't be able to see my home IP if we're all logging into a server.

Nick: Well so other than using dedicated servers, are there other things that game developers can do that you'd recommend to make it easier for people in your position to avoid these type of problems?

Ben: Another big problem we've been having recently is a lot of devs will use voice-over IP (VoIP) stuff and again with voice-over IP, you're sharing your IP. So if you want to have in-game communication with other players, which is awesome for making content - you're running around an open world like Sea of Thieves or in the Division and you run by someone and you're like "hey jerk" and whatever, you talk some trash and you create a narrative and you have fun in the game - but when you're doing that via a voice service that's kind of baked into the game the only to avoid someone yanking your IP is by turning it off. As far as solutions that I'm aware of, dedicated servers for PvP games is sort of the only way.

Nick: Sound's expensive.

Ben: It is expensive and that's why a lot of people avoid it. There's also some technical reasons why they avoid it, when you force everyone to log into a dedicated server you have to spin up an instance every time something happens. If, whenever you're listening to this, you look back to the launch of a game called Anthem, Anthem has dedicated servers but the loading issues is one of the biggest critiques of the game because every time you move your party from one location to another it has to spin up a server instance for you which takes time.

Steve: Yeah.

Ben: So games like Destiny will opt to save time by making everything peer-to-peer, because that's just a whole bunch of handshakes and then you're good to go, but you're sacrificing a little bit of security to make it less expensive and also run faster. So it's sort of like, you know, your hands are sort of tied.

Nick: Yeah, some serious trade-offs there.

Ben: Yeah.

Steve: So all this begs the question, what can you do? In your case, Ben, what were you able to do or maybe not do is a better question when it happens, when you've been hacked?

Ben: When your IP's been leaked or any of your personal data has been leaked, which is also something that's happened to me before, the best way to respond is to, believe it or not, first contract your IP and get your IP cycled or find out how you can do that. Most services they're either going to be able to do it for you on the phone, or they're going to tell you to unplug all of your equipment for up to 24 hours, whatever it takes for them to unregister your router's IP and then

reissue you a new one, and usually that will handle the IP situation. If your information has ever been leaked, or if you're threats or whatever, contact the authorities and start a log of this behavior.

Steve: Yep and that can happen at the state and federal level...

Ben: That's true.

Steve: ...they kind of have a concurrent jurisdiction in that regard. Sometimes there's cooperation between authorities and sometimes there isn't. So it can be quite frustrating and especially given the tech involved, it can kind of be difficult, because you would be the one educating the authorities on what happened and what may be needs to be the next step and they might not be there with you.

Nick: Right, I don't know that every law enforcement officer you deal with is going to know what cycling IPs means.

Ben: Yeah, I spend a lot of time trying to educate as many people as I can. The most visible thing that has come out of the gaming space is the concept of "swatting," which has at this point actually cost someone [his] life. And I think that's a good starting point if you're talking with the authorities, at least as a broadcaster, they're going to take you seriously because you have visibility. And if they don't take you seriously, my rule of thumb when you're talking to them, because I have an action plan with the local police here, I had an action plan when I lived in St. Louis that actually, I wasn't home but we got swatted and it prevented any problems happening with my other residents.

Nick: Before we go further, I just want to say some of our listeners may not know what "swatting" is.

Ben: Sure I'll break that down. So "swatting" is when someone gets your IP via one of the methods I was talking about, whether it's you matched with them in PvP or whatever, they pull your IP, they find out what the residence is that's attached to that IP, so they literally find out your address, then they call in a fake threat that requires response.

Steve: Armed response, right?

Ben: Armed response, yeah. Well sometimes people call in stupid stuff like just dumb crap. But when someone is trying to truly be malicious, they'll call and say I'm calling because I'm the neighbor of so and so who lives at this address, and they have people, I saw them, they have people in their basement that are tied up and being tortured, I'm not playing around. Or they're walking around with a gun, it's things like this, things that require an armed response that the police officers and the law enforcement with their defenses up because they have to. And this is where I was going with this, is when you speak to the police officers you have to understand that, you know, it's not every day that somebody comes in and says, hi I'm a person you don't know, you might be receiving a call about my

address that tells you I have someone in my house and I'm about to kill them. Which sounds like something that you would do if you were a really bold serial killer. So, what I like to say is, you need to make a plan that makes you safe because it is your life ultimately, someone has lost [his] life due to this.

Nick: You're talking about that event in 2017, when...

Ben: Yes.

Nick: ...there was a guy that was, he got in an argument with somebody else while playing.

Ben: Someone over Call of Duty, a Call of Duty match.

Nick: Yeah, right, you know, the most important thing on the planet. And then the other guy swatted him, the swat team comes out, and they ended up firing on the victim and killing him because he reached for his waist.

Ben: Yeah.

Nick: And all of it was over a video game argument.

Ben: Yes. Yes so that's the incident that I'm talking about, thanks for putting that out there.

Nick: Yeah, it's a mess.

Ben: Yeah so when you talk to police officers, you need to make a plan that's going to make them feel safe and keeps you safe. So I believe our plan in St. Louis was if they received a call about our residence, all of us we're going to go and we were going to sit on the driveway with our hands on our heads and wait for them to come and do whatever they felt like they needed to do based on the threat.

Steve: Wow.

Ben: And they were comfortable with that, you know, it's not something that a serial killer's going to say. They're going to be like yeah I will, you know, if you're actually trying to kill someone you're not going to sit on your driveway with your hands on your heads while the cops show up.

Nick: Sounds like something a serial killer might say.

Ben: Yeah, exactly, exactly.

Steve: How did you get started with that plan? Did you just contact law enforcement and say....

Ben: I set up a plan, we kind of contacted the front desk of the police office that was near us, you know, the station - that's the right word - that was near us and I just said we really want to meet with a detective or somebody, we just need to discuss some threats that have been happening and sort of figure out what we need to do. And, we talked about them, we were lucky we didn't have to do too much education, the officers were, oh yeah we know about that and oh well what do you do?

Nick: That's a good to hear.

Ben: Yeah, it's becoming a lot more visible now, especially after that incident.

So here's the conversation, because I want to make sure I say this, if you're listening to this and you're trying to have this conversation, show them this article, show them a video or two because there's plenty of them of people getting swatted, and just be like: look, I don't want to be the guy that's in the chair and I don't want you to be the officer that is standing behind me in this video because it makes everybody look bad.

Steve: Yeah, absolutely.

Nick: It's in everybody's interest to avoid these type of things.

Steve: Just this little education will go a long way.

Nick: So switching gears a little bit, let's talk about civil remedies like that non-criminal stuff. Steve and I were sitting around talking about the types of civil remedies that might be available, and it's kind of stark, it's not really clear what's out there because, even though this getting more common, it's still kind of fledgling issue where a lot of the law hasn't caught up. So you talked a little bit about, we had an episode of podcast on bugs and glitches in games where we talked about the Computer Fraud And Abuse Act a little bit.

Steve: And that's glitchy in of itself, so that's full of bugs.

Nick: Right and so we were talking about whether the CFAA is an option here and unfortunately, you know, the door isn't shut but it would be really difficult to bring a case under the CFAA for something like this, because among other requirements, that law requires you to demonstrate over $5,000 in actual damages.

Steve: Yeah, might be difficult in most cases to prove something like that among some of the other elements of this cause of action.

In Florida, we have another statute that may be helpful for some. Ben, I'm not sure if you're aware that in Florida there's this Computer Abuse and Data Recovery Act, "CADRA," for short. And it's purpose is to protect owners and operators of computers and computer systems - the caveat here being "used in business" - so it's for business purposes, stored on business computers, to protect those owners from harms caused by unauthorized access. So one of the things you can't do under CADRA is to transmit a program or code from a protected computer without permission, you can't traffic passwords or access information through which access to a protected computer may be obtained, which arguably in this instance may be could be IP, I'm not too sure about that. But important here is that the statute doesn't have this minimum threshold requirement that the CFAA has.

Nick: But it also doesn't protect individuals, right?

Steve: Right, so the trick here is if you were maybe gaming in your professional or in your LLC capacity, versus your individual capacity, maybe there's something there. Whereas if you were just an individual gaming, that's obviously a big thing that this particular act doesn't protect individuals. Other than those things, maybe one could look to tort theories, tort being like....

Nick: An intentional wrong act.

Steve: Right, right but those are harder to prove, especially when you don't have a statute that's kind of on point. So that's it, and it kind of creates this big gray area where you're left kind of like you're trying to do your best, it almost happens to everybody, it's not a matter of if, it's a matter of when.

Nick: Nowadays, yeah.

Ben: Yeah.

Steve: In Ben's case, you take as much security measures as you can and even then it still doesn't work. So what can we take away from this conversation to kind of wrap all of this up and to put it into context? Well, I'll start. First, we can build awareness, which is kind of a big message that this podcast episode about.

Nick: Hey, it's what we're doing here today.

Steve: That's right, and you help those playing games be smarter gamers when it comes to cyber security. And in addition to that, we can talk to law makers about some of these issues to build awareness that they exist and also that there may not be the areas of redress that there may need to be in terms of maybe instead of this act applying only to businesses maybe we can extent to individuals in the same capacity or in another one.

Nick: Well there's also, you know, you want to protect yourself as a gamer and practice safe cyber-hygiene. And Ben, I'm sure you know all about this, it involves don't use the same password everywhere, use strong passwords, don't share your password, use two factor authentication. Do you have other security tips?

Ben: Yeah, I think that to take things a step further, if you can, using something like Google Authenticator on any locations you can is actually fantastic. That's been a final line of defense for me before and saved my a--.

Steve: Mm-hmm.

Ben: And I know not a lot of mainstream sites, I know Twitch doesn't, if it has it because it might, it doesn't make things painfully obvious. Putting as many layers between you and someone else is the best thing that you can do.

Nick: It's like an arms race, right?

Ben: Yeah. So, it's putting as many layers between somebody else and you is the best strategy. You have to walk to the line as a content creator between ease of access to you and your level of security comfort. I'm more risk taking than others. I have a lot of one on one interaction with fans. I accept an answer like every Instagram DM that I've ever received, things like that, because I think it's important. And as you said earlier, I give a lot of advice, so I like to make sure that I'm doing that as much as I can and provide as much access to myself as possible. But at the same time, I've made a purposeful decision to only use that platform and not Twitter and everywhere else. Make sure if you can, and it really depends on the State that you live in, try to get your address hidden. If you use an LLC, use something that is not obvious. Like if your name is Twitch.tv/Paul, don't make it Twitch Paul LLC. Think of something really random, like Light Bulb Umbrella Soundboard LLC.

Nick: Is that yours?

Ben: No, it's not. But that's actually a vulnerability that we all sort of realized very recently at our, I guess you'd call it a holding company that runs all the stuff that we do, because people knew the name of that company and then we were like oh crap, well it wouldn't be hard to figure out the names of our LLCs, and like oh crap, those are our home addresses. Well, I need to change everything.

Nick: More layers.

Ben: Yeah, as many layers as you can, try to add obscurity where you can just to make things a little bit harder. Ultimately, if somebody wants to hurt you online they're going to figure out a way to do it, but most of the stuff that is happening in the gaming space is somebody who is really mad

temporarily and acting out, and if you put 24 hours of work between them harassing you in a meaningful way, in an illegal way, and the incident that's inciting it, most of them are going to give up. So that's kind of my strategy.

Steve: One last thing before we leave the individual, I think education on clicking on links is huge. And it's as simple as hovering over a link to see what that link is, usually if it's HTTPS that's a good sign. Sometimes it doesn't have that, but if it's like something weird and you don't trust it, if you have an IT person you can send it to, or just find access to wherever you're going in a separate way. Just, be careful and that's easy stuff that you can do to save you from some really bad headaches later.

So let's switch gears real quick before we finish for developers, what could developers maybe do - and this is coming from two lawyers talking about this - but things I can think of is building security features in the games. Ben has just mentioned Google Authenticator, that's a type of two factor authentication that exists where it doesn't already exist inside a game. So if you put that in the game or the program, that's a good way to boost the security of that offering.

Also consider hiring white hat hackers, companies going out there and purposefully hacking but with the intent of finding holes in the cybersecurity of whatever we're talking about.

Nick: That would be a fun job, right? White hat hacker.

Steve: Exactly, you know, I'd be interested if they used Red Hat Linux to do that white hat hacking. That was probably a really dated Linux joke.

Nick: At least four people will get it.

Steve: The last thing I can think of is to be prepared when things go wrong. We had a lot of examples of being prepared when things go wrong here tonight, today in this podcast. There are other ways you can be prepared, like having a data breach incident response plan in place, which lawyers and executives can put together. I've been involved on a lot of those. And they really help, because it's literally you pick up this paper and it walks you through the process of we've just got breached, what do we do? Okay, you categorize it, is it a red, is it yellow? It's just good to have when you're in the red.

Nick: Right, and just like Ben said, you've got to start thinking about this stuff before it happens, once it happens it's a lot of times too late.

Steve: Well, Ben, this was a lot of fun, we are out of time, thank you so much for joining us on the podcast. Before we go, I'd just like to have you put a plug in for wherever anybody can find you so where can we find you for people looking to connect?

Ben: If you want to connect with me anywhere I'm Professor Broman on Twitter, Twitch, YouTube, Instagram, Snapchat, anywhere.

Nick: Do you want to give us your IP too?

Ben: No. So that's the best place to connect with me. If you're interested in any of stuff that I do, I'm the charity director for an event called GuardianCon. We raise money for St. Jude's Children's Research Hospital, so if you're interested in getting involved with that you can reach out to us at info@GuardianCon.co. And if you're interested in having delicious coffee, I also own a coffee company and you can check that out at KingsCoastCoffee.com

Steve: Congratulations on all that stuff, that's awesome, thank you so much for sharing your wisdom with us today, we really, really appreciate it.

Nick: Yeah, that was great, thank you so much.

Ben: Thank you.

Steve: So, Nick, I have nothing else to add, I think we laid it all out, unless you have anything further.

Nick: That's all we've got today but keep your eyes out for other cool episodes of the podcast where we touch on issues with respect to video games, law, and business, until then, game on.

Steve: Game on.

Related Practices

Cybersecurity and Privacy
Esports and Electronic Gaming
Media, Entertainment, Music & Sports