Interview A2

Date: 15. May 2025
Duration: 17min 16s
Language: English

Speaker:	Text:
I:	So, you have reported that you experienced some incidents. Can you tell me again about those incidents with as much detail as you can think of? (0:12)
A2:	Yeah, so, I help as part of a team to manage and provide a free community resource through a third party trading website. So, you'd be able to trade for in-game items with in-game gold and it kind of matches you up with people looking to sell or buy. And it's quite often that we'll be under DDoS attacks, largely from (...) proprietors of real money transaction sites. So, those are sites where you pay real money for game items, which is against the game rules. But they clearly don't like that we're trying to (...) be clean, as it were. So, it's not often that we'll get a DDoS from typically out in, I think, largely data centres in Taiwan, stuff like that. It's a (...), yeah, so, that's the main incident. But then we also, (...) through moderation of that website and our community server on Discord, we'll often find that users will pay for in-game items or gold and then find out that they're not getting those items. So, they are out, out of the money, which is one reason we are quite strongly against it, yeah. (01:28)
I:	That's quite interesting, because when I read your response, I thought that these were, like, normal people or customers who say, "I don't like that you don't take real money for those transactions". So, they are DDoSing that or using these DDoS attacks against you to enforce that kind of (...) policy. So, you think it's mostly other websites who see you as competition? (01:55)
A2:	Anecdotally, because some of them have spoken to me directly. Typically you have a studio. So, you'll have a, almost like a, scam call centre, in a way, of individuals who work on behalf of a website or group. And those individuals will attempt to use our resources for their own good to (...) to get customers effectively. And so, when we prevent them doing so, we get not just threats of DDoS, but we do see an uptick. We're quite well protected now, but in the early days, it was more than just a threat. But, it's a, typically, (...) I don't know for absolute

	certainty, it's a specific studio, but I know individuals that work on behalf of those studios tend to organise that, yeah. (02:45)
I:	I'm really interested in how you personally (...) think about those attacks, how you percept these risks of the attacks. Is it something you say, well, it's just (...) common annoyance, or do you think that's more like in a blackmail way of enforcing something on you? What's your perception of that attacks? (03:13)
A2:	It's definitely a nuisance (laughs). I wouldn't say that there's a material impact such, just because of the protections we have. I, I'm not a developer, I'm more of the community side of things, so I don't know the ins and outs, nor would I try and speak on behalf of those who know far more, but from what I understand, it's, you know, like a baby having a tantrum. It's not, it's no longer consequential. (...) It's just, I guess, personally, it's upsetting to think that people would (...) try and take down a resource like that because they can't take advantage of it as a community member, rather than a (...) a member of the site, yeah. (03:59)
I:	Ah, okay. So you think it's something you have to deal with because that's how it works? (04:05)
A2:	I think it's the price of being (...) good, I suppose (laughs). (04:12)
I:	Have these incidents when you say it's (...) it's not a good feeling to have people attack you, is there some form of attacks that ever (...) changed your emotional state at that moment, like annoyance or rage? (04:30)
A2:	I think I've quite thick skin now, I think it glances off, I would say. I think there are instances on the community side of things, largely with the Discord server, that maybe sometimes can get under the skin a little bit when they (...) you know, there's always this fear in the back of your mind that they might find out who you are and dox you and make complications in your real life. So there's an element of that. But, you know, I think if you put yourself into a voluntary position to try and cultivate a community, you, you (...) accept that there are risks associated with that and tend to downplay them, I think. It's, I'd rather me than someone else almost, so, yeah. (05:14)
I:	Do you only operate your website or are you a gamer yourself? Do you play video games?

	(05:22)
A2:	Yeah, so I'm (...), the only reason I volunteered to help the site and the community is because I'm part of that community and it's kind of like I was hanging out there anyway, I stepped up and (...) tried to kind of help people have the same experience I had. So it's, you know, yeah, definitely. (05:43)
I:	Did you ever notice or experience any incidents in-game yourself? (05:48)
A2:	Yeah. I mean, particularly if I'm playing, like a shooter game and we're doing quite well, you get, you know, the obvious (laughs). Some people are unhappy to see your success, I think, in those types of games where you have a competitive element, definitely. It's rarely more than verbal abuse, thankfully (laughs). (06:08)
I:	So no case of hacking your account or something like that? (06:13)
A2:	I've not had that personally, no. I like to think I've got it all pretty locked in and locked down, yeah. (06:21)
I:	You know, you're kind of in a special spot for me, interview-wise, because you're not only playing games yourself, but you are also operator or distributor on a website. (06:36)
A2:	Yeah. (06:37)
I:	Which is another perspective that's really interesting. What security measures do you take (...) also while gaming, but also on your website to keep yourself safe and every of your customers safe? (06:51)
A2:	So personally, it's, you know, two-factor authentication, make sure you're using different passwords, all the (...) the bread and butter. I don't think I could divulge the measures we put on the site, just because, you know, if (...) if people find out they can work around them. But it's, (...) we've been using something called OAuth, which is a third-party authentication. So there's nothing we hold directly that could possibly lead to (...) harm for anyone using the site, because it's handled by (...) the Battle.net service, which is the login service for Blizzard. So it's, yeah. (07:30)

I:	All right. So you're enforcing those two-factor authentication, or is it just an option for your customers? (07:37)
A2:	What they do is up to them. I think everyone has to manage their own appetite for risk. Even on the Discord, we don't. There are options to say you can't join unless you have this set up, but it's (...) not typically the case. Yeah, it's, you know, you can't really handhold people to an extent. And I think a lot of that comes down to the individual. A lot of the time, we do get, through moderating, a lot of the moderation we do are people who've had their accounts compromised because they've clicked some (...) dodgy link. So we'll (...), we'll ban them, and then alongside the ban, they'll get a brief message on how to protect themselves in future. So there is, there is some element of education, but it's one of those things I think you only learn when it happens to you (laughs). Yeah. (08:25)
I:	If those people click on links, do you think that's someone with a phishing attack, like cloning your website to make it look authentic? (08:35)
A2:	So we don't get it on the website, at all, because the chat is very limited. But on the Discord server, yeah, it's typically, you know: “Oh free Steam gift card, click here to blah, blah, blah”. And then they log in thinking it's Steam, but it's actually, you know, a phishing site effectively, yeah. (08:56)
I:	Are you, in most of the cases, able to help them and support them to get their account back? As if some (...) trade they had, that was authorised because someone else triggered it for them? (09:13)
A2:	So that's (...) the beauty of: We're completely third party. So there's no tie with the game directly, so (...) all the site does is facilitate a chat between two players based on a listing they've made or so. In-game is completely different. I wouldn't be able to speak to direct in-game harm. I think on the Discord server, where it's our community server, we have kind of a two-part approach to it, which the first is to remove their access to the server, because then they can't spread the link onwards. Obviously stopping other people doing it and then saying, hey, appeal this when you have changed your password, set up multi-factor authentication. And it's, you know, (...) a learning moment, I think. (10:00)

I:	With your experience with especially DDoS, but also then those cases of account theft or phishing from your customers, can you give me your opinion on the most relevant security risks when it comes to gaming or using gaming-related services like yours? (10:22)
A2:	I think, the key (...) the key is making sure that you keep your kind of, (...) your other life separate. You know, use a pseudonym. Don't use your real name. Don't let people know who you are beyond your persona on the internet, because I think (...) when it comes to things like phishing or like verbal abuse, these things, their surface level, the stakes are really low, because all you have (...) to stake is, say, your account or your state of mind, I guess. But if you let on more than you should, you perhaps open yourself up to real-world risk, you know, if they find out your full name or where you work, or.. So I think, yeah, the key is just being sensible and making sure you (...) you don't let people know who you are. Even if you trust them. I think a lot of the times, a lot of the worst instances I'd imagine are social engineering, where someone you trusted or you trust then, you know, backstabs you. So it's just being able to limit that harm through being more vigilant about who you, what you reveal about yourself on the internet, I would say. (11:40)
I:	So it's mostly about privacy for you? (11:43)
A2:	Absolutely, yeah. Privacy. (11:45)
I:	Can you give me (..) any information about communication with official developers or official game companies you have (...) noticed, either with your website or for yourself regarding some kind of security risks they want you to be aware of? (12:08)
A2:	No, because we're (...) we're completely, the site's completely non-profit, community-run, third-party. So there's no (...) no relation whatsoever to any official developer. (12:20)
I:	Okay. So Blizzard never contacted you regarding anything? (12:24)
A2:	No. I think we, we uphold their terms of service just because it makes sense to do so (...) as part of our own terms of use, but it's yeah, completely separate, completely severed, so..

	(12:36)
I:	So would you think it would be helpful to actually get some form of communication from developers regarding some things? (...) If something in their games poses the risk of, I don't know, account theft for example? (12:54)
A2:	Potentially, I (...) I think they have their own processes in place. I think they (...), they have their own launcher and their own means to communicate any risks. I think (...) I think there's a beauty in being separate to be honest, it's (...). I think there are different things you can do, depending on what your motivations are and I think when you're a volunteer team providing resources or cultivating the community, that's completely different to when it's, you know, your job, because there's more at stake. So yeah. (13:25)
I:	Right, that were my questions, but I have one more for you specific, because (...) you were one of only two persons who actually replied to my invitation for that interview. With your case specifically, (...) I would really like to know something about your background. So why were you interested in taking part in the study? (13:57)
A2:	So I, I was an undergraduate and I (...) I pretty much ditched my initial dissertation thesis because I couldn't get the numbers to do it. And it just (laughs). I can't remember her name, but someone posted a link to their survey. It related to this. And one of my moderators struck it down thinking it might be, ironically, a phishing scam of some sort. But I reached out and it seemed legitimate. And I thought, actually, no, I'm going to pay it forward. And I'm going to try and platform it. Let's see if we can avoid anyone going through what I did as an undergraduate who had no one respond to any surveys they sent out (laughs). (14:44)
I:	So it was mostly about helping me, but not anything regarding cybercrime where you feel is really important or "I need to talk about that"? (14:56)
A2:	Yeah, there's another element. Obviously, when you (...) do something, when you are curating a community server of half a million people or providing resources, I think everyone benefits to knowing the real risks. And I think that distinction between yourself and your persona, I think if more people were aware of (...) the damage it could cause, the better. And I think, you know, if you can back that up with a study, obviously, people tend to take it a little more seriously. So there's an element of that too. So I

	wouldn't (...) have partaken if it wasn't interesting personally as well. I appreciate it, so likewise, yeah. (15:39)
I:	Well, that was that. Anything in the ending you would like to (...) talk about or give me some other topic that's on your mind regarding the study or cybercrime or your website, anything you would like to add? (15:57)
A2:	Nothing in particular. I think (...) my interest with it is, is ignorance. Personally, I think the majority of people who are (...) victim to this kind of flavour of crime, in my experience, they've either welcomed it in through poor privacy and security, through taking things too personally or through (...) kind of provoking it a lot. So in the same way that we provoke the rage of (...) RMT studios by being good, I think a lot of people perhaps, if they (...) if they go like for like when someone calls them a slur or something, you're kind of escalating that behaviour. So I think for me, it's, yeah, I think ignorance, as brutal as it is to say, I think is at the core of a lot of these issues and allow bad actors to thrive in a lot of cases. But it's a shame at the same time, you're only ignorant because you kind of don't expect it. You know, when someone offers you a free thing, you don't want, your first response to be that's terrible. So yeah, very interesting. I find it very interesting. (17:12)
I:	All right, then thank you very much. (17:16)