Interview A1 - Translation

Date: 07. May 2025
Duration: 27min 42s
Language: Translated to English

Speaker	Text
I:	Okay, you indicated in the survey that you have already experienced cases of cybercrime. Can you tell me about those cases again? (0:10)
A1:	Yes, I can, as I was affected by a security incident myself. It basically happened like this, I woke up one morning, I was ill at the time, so I wasn't on my PC much at the time, or at the time, and I noticed that my Steam account was logged out and wondered about it and then logged in again. And then, yes, my profile picture was changed and my name was different. In short, someone had gained access to my Steam account. Even though I have a second factor via Steam Guard. But it was simply deactivated or no longer active, apparently. However, I was still able to regain access to my Steam account via the Steam App. In other words, the account was not lost. The problem was that in addition to the, shall I say, cosmetic shop coins that you get from Steam, there were also In-game purchases were made via my linked Paypal account in the amount of 200, approx. 200 euros. And purchases were made that then gifted Steam games to other accounts. Then I basically went there and first tried to undo everything that was possible, to change passwords. And then I started thinking about what else is or could be corrupted. Shortly afterwards, my Discord account was also affected. And it then sent a spam message to all contacts, in all chats, in all servers that I had access to, in every single channel with, with a Steam gift card for, I think, 20 or 50 euros,I can't remember exactly. With a link that would probably lead to further victims if someone clicked on it. The problem is, I've never clicked on this link or a similar link before. This means that my credentials must have been become public somehow. The problem is that I believe that in the in the past, my Steam account and my Discord account had similar passwords, even if different, but the same e-mail address. That will probably have been the case. That was still the case back then. Yes, afterwards I noticed that, where my e-mail address was also used

	and a similar password, not the same, definitely not, (...) my Humblebundle account was practically crawled once and all Steam keys or all keys that were not yet claimed were also automatically read out, because they were all claimed and then probably drifted away to somewhere. (3:39)
I:	Did anyone help you to solve the incident then? (3:43)
A1:	Yes, I called and wrote to Steam support. They were very helpful as far as fixing the damage. When clarifying the whole thing, they insisted that the security leak had supposedly existed for over a year. I then searched my machine again and couldn't find any conspicuous programs, processes or entries for the time being. (...) And the accesses (...) could or probably did come via my PC itself, which is why I couldn't explain how the Steam Guard could be bypassed or circumvented. Steam support didn't want to tell me that either. They were very insistent about not telling me what was really going on. I was reimbursed for the loss of 200 euros in credit. (...) And yes, all the other purchases were practically reversed, apart from my cosmetic purchases. Which then just the, yes, the little points that you get with the purchase of any games, where a few had accumulated over the last few years, which hurt a bit, but in the end it doesn't matter at all for now. From my point of view, because I've never used this shop. (5:13)
I:	Okay. But that means, with Humblebundle, your claimed keys, were they restored by Humblebundle or by Steam or someone else? (5:23)
A1:	No, I have to admit that I didn't approach the support again. Because I thought to myself, yes, at the end of the day it was my own stupidity. And then I went there because I thought to myself that the keys had probably been read out in order to be offered on some reseller sites, like G2A or something else, where you suspect that these could often be stolen keys anyway. (...) In short, I then went and wrote all the keys that were then opened or read out to my Steam account. That was an evening when I did nothing but claim games. And I went back through the months and months, (...) actually years, that I've had Humblebundle. (6:19)
I:	Those were already good descriptions. Which game-related services or platforms have you generally had good or bad experiences with and why? (6:29)
A1:	(...) Bad experiences? (groans) If I were to say bad experiences in terms

	of performance, I would say Uplay. But that's more down to their infrastructure and the game design in general, because the online requirement for single-player games is an absolute joke. That's the only negative experience. I've only had one real security incident in this form so far. (...) And I have to honestly admit that due to years of experience in this professional field, I would say that I was able to work through the whole thing in a very structured way. And so (...) I've added a second factor wherever I've neglected it in recent years due to laziness. (7:22)
I:	I'd be very interested to know, even though the second factor obviously failed with Steam, didn't that somehow deter you from continuing to use it or using it on other platforms? (7:35)
A1:	(...) No. So clearly no. Even if there is possibly a vulnerability in Steam, that doesn't automatically mean that this vulnerability also exists with other providers. And at the same time, you have to remember that (...) just because a vulnerability exists doesn't mean that everyone can exploit it. (...) And (...) not using the second factor is even more negligent than using it and then falling for it or becoming a victim of such an attack. Because you can only do your best to protect yourself and then you can always say and talk to the support team properly: Hey, I have taken the measures that you offer me as a user. Now it is in <u>your</u> interest to help me. (...) Instead of being negligent and saying, no, an e-mail address or a password is enough. Then you're basically giving the business partner on the other side enough cannon fodder to say, yes, but if you would only had the two-factor service that we offer here, then this would not have happened to you. (...) Because it can always happen that somewhere in the world, databases of user data and passwords are stored somewhere, get onto the Internet etc. pp. This happens every year or in larger quantities every few years. (...) And these lists usually result in a (...) yes, let me say, user profile, which is not necessarily coherent, but if you try out usernames and passwords on different services, you will inevitably come across hits at some point and you can probably have success with the combination on other websites, because many people (...) or most people, I would say, are so lazy, and unfortunately I have had to count myself among them for a long time, and use the same passwords and the same (...) e-mail addresses for, or usernames for, other websites....) or most people, I would say, are so lazy, and unfortunately I have had to count myself among them for a long time, and use the same passwords and the same (...) e-mail addresses for, or

	usernames, for their accounts in order to be able to log in more easily. (...) So in short, the consequence that I have drawn from this for the time being is to consistently use two-factor, to write the whole thing with the recovery keys in my Bitwarden or in my Keepass, so that in the worst case I can reset it if something happens to it, because there is also enough two-factor, or there have also been cases in the past where the service or the, (...) the service owner of the second factor also stops the service, then of course you have to be able to remove it again. (...) Or you might forget the password for it. (10:37)
I:	Aside from the two-factor and the dedicated passwords, are there any other security measures that you personally use to protect yourself while gaming? (10:51)
A1:	To protect myself while gaming? Basically get no downloads from just somewhere, from some sites. Always get it all from secure sources,, if (...) basically, it's actually switching on your brain first. If someone offers me something for free, I'm usually the product. At the same time, I already did that beforehand, (...) I use an adblocker to prevent any occurrences, i.e. forwarding and so on, so that I'm not simply forwarded somewhere. At the same time, downloads are uploaded again to Virus-Total or similar to check them. (...) So, to check again, what is really in there, are there any analyses of it, because usually it is enough to upload the hash of the file and then, yes, you can see quite quickly whether there are suspicions or a suspected case of a virus, a Trojan, etc. pp. (...) You can immediately assess whether I really want to open or run this ZIP file or possibly this exe on my system. (...) I would say that this is actually relatively secure from the user's point of view. But there is never one hundred percent security. (12:03)
I:	Have these security measures or your security behavior in general changed as a result of the incidents you experienced? (...) Has anything been added as a result? (12:33)
A1:	Of the measures I already take on a regular basis, not much, except for the consistent use of the second factor and increased splitting or individual passwords for individual services, which I then write in my Bitwarden accordingly.

	(12:53)
I:	You've already taken this away a little, and that is, what would you say, where do you see the responsibility when it comes to being safe in the gaming world? With whom and why? (13:08)
A1:	On both parties. On the provider and also on the consumer. It cannot be that the provider has to force all options in the worst case. But if this is the case, then the service concept is always there, which may prevent security features or only offer them voluntarily. On the other hand, if the user is already using everything, then the provider is also responsible for replacing it if necessary and undoing the damage, where you have to say that Steam has reacted in a good way. They didn't make a big fuss out of it. They refunded me the money and repaired the monetary damage for the time being. (...) I've now lost confidence in their two-factor service, yes, but not using it would be negligent. (14:02)
I:	Have your experiences with the attacks ever influenced your emotional perception of the game or the platform in any way? (14:12)
A1:	So, (...) it was, at the time it was quite an emotional, (...) well, it was an emotional carousel at first. Because, (...) to feel this pressure in your chest when you realize, oh, (...) years of investment in something are being lost. (...) Or could be lost. Or someone simply has access to my things. Someone from outside, who (...) definitely can't or shouldn't have access to my things, (...) suddenly has access or is suddenly in my account. They can read my messages. They can see my games. They can (...) see all kinds of things I've done there. That's a deep invasion of privacy for a start. It does something to the person in the sense that (...) you first fall into a state of shock and have to think about it and calm down again. What can I do at this point? (...) And then you actually have to act quite quickly, but at the same time not panic. So the days when this happened, I was sick and exhausted, but I definitely didn't sleep well. And it was not because I had a cold. (15:29)
I:	What is your general perception of cybercrime risks or dangers now when playing games or using game-related content? (15:40)
A1:	My general perception is that modding basically opens doors first and

	foremost. Just like (groans) illegal downloads of games. (...) This can always go hand in hand with malware. That's nothing new. It was around 20 years ago, before platforms like Steam or anything else existed. You always had to be careful what you put on your systems. Basically, I would say that the biggest gateway is still spam or (...) phishing. And (...) not so much the games themselves. (16:25)
I:	In other words, your perception has not changed as a result of what you then experienced yourself, but (...) is it the same or has it changed as a result? (16:39)
A1:	Not really, I was already aware of a lot of things, because something like that has happened in my environment before. At first I couldn't believe that (...) because it was still a teenager at the time. That was the son of my girlfriend's godfather. (...) He said, yes, my Steam account has been hacked. (...) And gone. Then I thought, yes, what kind of link have you clicked on again? Because young, pubescent, (...) you just have to catch yourself in a, let's say, careless second, then you click on things. (...) But he was clever enough and had a second factor with Steam. And it seems to be a vulnerability that has been open for a long time. (...) Which doesn't necessarily speak in favor of Steam in this case or for this second factor as a security factor. (...) So to cut a long story short, no, my perception of this hasn't really changed because I was already aware of many of the risks beforehand. (17:47)
I:	But you've never been affected yourself by the risks like modding or illegal software downloads that you've just mentioned, have you? (17:56)
A1:	In any case, it hasn't happened to me yet. (...) It must also be said that, as far as I know, it has never happened to me. (...) It could also be that at some point during a LAN party in the 2000s I installed software on my PC that was definitely harmful. But that was also at a time when I, I don't want to say weekly, but every few months I (...) regularly reinstalled Windows, now I have to think about it for a moment, XP. (...) Because I also played around with the system a lot and also deleted things that I shouldn't have deleted and shut down the system from time to time. So as far as I know, it didn't happen. I can't say for sure.

	(18:50)
I:	Can you tell me anything about communication or warnings from official sources that you have received or heard? (19:01)
A1:	Honestly? (...) I think this is a topic that is hushed up on many platforms and not even communicated in a big way. But I also have to say that I'm at most via the communication channel e-mail, as I avoid social media. In other words, if someone posted something on some Twitter page or now it's X, (...) or somewhere else, I wouldn't notice it anyway. So, (...) in the launcher or in the launchers themselves, I've never experienced a security warning or generally a (...) warning about security incidents. The only thing I have experienced is a request, I think it was Blizzard at the time, who asked me to use their own authenticator app, as a practically mandatory second factor. (...) That would be the only thing I could think of. (20:03)
I:	Okay, and among the experiences, then what is your opinion on the effectiveness and extent of such official communication regarding security risks in games? How effective and how extensive is it? (20:17)
A1:	So, you have to make a distinction here. It is usually not the game developer who is responsible for the security of the platform, it is the provider of the respective platform. In most cases, the game is left out of the equation. (...) If I get it from a platform at all, then the question is, how else do I get it? (...) I have to be honest, (...) I can't answer that. (20:50)
I:	What kind of information or help would you find helpful in order to be informed and protected in the gaming world? (20:57)
A1:	The nice thing about open source, or rather CVE in particular, is that vulnerabilities are made public. Mostly in a responsible disclosure procedure, where you can say: (...) Hey, they talked to the manufacturer in advance, they have the time to fix this vulnerability, and then this vulnerability is published. (groans) That would actually be the best thing. But I think that as things stand at the moment (...) we are a long way from the platforms dealing responsibly with security vulnerabilities and, if necessary, publishing them and also informing users that this was once an issue.

	At the same time, the main problem is often that users do not take adequate, or only insufficiently adequate, security measures for themselves. (...) I don't want to know how many people in my environment are still using the same passwords as ten years ago. And in the meantime, in the last eight years alone, we've had a lot of data breaches, I think (...) major password leaks have been known since 2017, which have definitely affected me as well. You could well check on the Have I Been Pwned website (...) to see whether you were affected, in which leak you were affected and on which platforms. (...) But that had little to do with the actual game provider industry. (22:45)
I:	When you say you know people who you think are still using the same passwords they used ten years ago. (22:52)
A1:	Yes. (22:53)
I:	Can you imagine certain behaviors or motivations in players that would make them vulnerable to cyber risks? (...) Or can make them? (23:04)
A1:	Basically first of all, and this applies not only to players, but in general, laziness. That's the main thing that makes people vulnerable in terms of security. (...) Because it's always easier to enter a short password if you have to enter it. And in the best case, it's still stored somewhere on the device so that you do not have to enter it in the first place. (...) Because then you can start straight away and consume the game. And (...) I think that's the biggest behavior, or the biggest problem, is that most people do not want to deal with security at all. For one thing, they do not understand it or can not understand it. Simply because the in-depth knowledge that we both have does not or they cannot understand at all how attackers can and do act in this time. And exploit it regularly. That, as soon as they even have access to your cache, they may be able to obtain session cookies, which they can then use to gain access. Without them knowing the passwords. (...) This is all possible in principle and is still a variable attack vector if you have strong passwords. A strong password is no good if an attacker gets access that way. And I think the main problem here is that most people, most people are either lazy (...) or the main problem is laziness, and most people simply do not

	care. So how many times have I heard this phrase, never mind, what do these people want with my data? What do they want with it? (24:54)
I:	But if I understood correctly, you were referring to everyone in general, so that's nothing... (25:01)
A1:	This is general. (25:02)
I:	Game specific? (25:03)
A1:	It has nothing to do with players, for a start. Players, I would say in most cases it is just laziness. (...) For many other people in the general public, it is ignorance. (25:14)
I:	I see. So you would say (...) or I don't know, can you think of different types of incidents that are specific to gaming? Or that occur more frequently in the gaming sector, if you exclude it from the general? (25:36)
A1:	Things that occur more frequently in the gaming sector are probably, yes, account theft. (...) So that people really do gain access to e-mail addresses and also to the accounts in order to then actually change the accounts to another e-mail address in order to gain permanent possession of this account. I can well imagine that this really is a widespread problem. I don't know. That's just my opinion. At the same time, I still think phishing is and remains another problem, because I think people often still have a chat open somewhere when they're playing and, in the worst case, have some general chats or larger Discord communities there, where there are at least one or two stupid people who probably click on a link like that for fun or out of ignorance and then become victims of such phishing attacks, where they may then also be attacked via a Session cookie steal (...) as access may be gained. (26:45)
I:	Okay, that's all the questions I had. Now, just to conclude, would you like to say anything else, add anything? (26:57)
A1:	Basically, if it is mentioned in your work in any way: (...) If you are affected, keep calm, systematically look first at which accounts you have, which is

	important, that you perhaps even have a list in advance, for what, which accounts you have, which, at least which e-mail addresses are somehow linked to them and where I may have the same passwords. This should always be avoided for the time being and, even if I have become a victim with a second factor, use the second factor. (27:35)
I:	Okay, thank you very much. (27:41)
A1:	Yes, you are welcome. (27:42)