# Transcription expert 9

Duration: 46 minutes

X: Could you explain to me what a VPN is?

Y: Eh, yes. VPN eh, from what I know I think it is a sort of private network and it is used within [the professional services firm] as well, so we use [the VPN of the professional services firm] to log into a private network that is operated, managed by [the professional services firm]. And from what I know it is, well, is separates the private network with the external network, so the big bad internet and it makes the internet connection more secure and it allows for eh, well, services that are only allowed if you are logged onto the private network. That is my understanding.

X: Okay. And what kind of services do you mean?

Y: Eh, services such as, we have some [an internal page] for example, that is only accessible if you are connected to eh, [the VPN of the professional services firm], so that's [0:02:28 till 0:02:46 has been omitted]. Yeah, I think that’s it.

X: Okay. And you describe it as a private network, what do you mean with private?

Y: Eh, as in not connected to the external eh, internet, I suppose. It is like a shell around your organization and inside the shell all the data traffic is of course not linked to the outside world and the data traffic inside it is managed as well by your own organization or the third party who is managing this internal network. Yeah, that's my understanding of it.

X: Okay, and eh, with manage, in what sense do you mean that?

Y: Eh, some sort of restrictions, like probably I cannot visit all websites, or they can also manage, well, what websites I visit and eh, what data I send out or download probably. I have not met anything like this eh, but yeah, I think those are the possibilities.

X: Okay, and you said that it makes your connection secure, what do you mean with secure?

Y: Eh, well, from what I know, if you normally log onto the internet, you of course you have eh, you log in from your outbound network, so you have your own IP-address and eh, when you visit a website, it is like two servers talking with each other. And eh, yeah, they can see my IP-address and eh, if I am more technical maybe you can also view their IP-address. And if you use a VPN, I think that is like an extra wall in between, so my connection goes via the VPN to this external source. So, they cannot directly view what is my eh, IP-address, among other data. I am not so sure what other data they can't get to, but pretty sure about the IP-address part.

X: Okay, and you mentioned a server, what is a server?

Y: O, good question, haha. Eh, basically eh, a device that regulates data traffic going in, going out. Eh, yeah, it is able to store data, it can manage the eh, also the internet traffic going in and out, I don't know. I don’t have a good definition for what is a server.

X: Okay, and in what sense does it manage the traffic?

Y: Sorry, can you repeat?

X: In what sort eh, in what kind of sense does it manage the traffic?

Y: Eh, you mean the, a server or the VPN?

X: The server.

Y: Does the server manage traffic, I don’t think the server does it by itself, right. I think it is either VPN or the person that manages the VPN or some sort of firewall that can manage traffic. I don’t think that is something that happens in a server, right.

X: Okay. Eh, that makes it a bit more clear what you meant earlier. Eh, why do you use a VPN?

Y: I think I touched upon that briefly already. Eh, well first off to eh, for an organization like [the professional services firm] it is good to identify your eh, employees, that they are part of this private network, they can identify themselves. And by doing that eh, you can then provide the extra services, such as [0:06:44 till 0:06:47 has been omitted], so examples I gave before. Eh, and other than that, also the secure connection of course. It helps that you cannot visit for example weird websites or download malicious software. Or at least, that's a bit more regulated than not using a VPN. Eh, and of course the story about the IP-address that it's masked, that also offers some security benefits, from what I know. Eh, yeah, I think those are the prime examples.

X: Okay, what would be the benefit from masking your IP?

Y: Eh, good question haha, I am not too technical in this area. I do know that eh, if you know someone’s IP, you can eh, have targeted attacks on that IP. You can eh, how do you say that, I don’t know if for example DDoS attacks are related to this. I give you our- If you know an online address and you want to target this with a hundred computers, then you're able to do so. Eh, yeah, it is the identity of your network, your internal network. I don't see why you'd want this to be exposed to the outside world. Especially if I am logging in from home right now and I am working, would it make sense for eh, the connections I have in the workplace to have my personal IP-address, so to say.

X: Okay. And do you use a VPN for any other purposes?

Y: Eh, yes. Eh, some things I can think of are for example some services that we use as eh, just at home. Eh, for example [country] has a very strict policy for [social media platform] for example, it blocks videos. Eh, and if you can use a VPN to eh, mimic you are in a different location, or at least shield that you're in [country], then maybe you can view other videos. Eh, I think that is one of the applications for a VPN. Eh, yeah, yeah, I think that is it. Other than the security reasons of course that I already mentioned. Those are, yeah, strong reasons to use a VPN as well.

X: Yes, and do you also use the [the professional services firm] VPN to change your geographical location?

Y: No, no.

X: Okay. Eh, then another question. What actions do you take to create a VPN connection?

Y: So, for me, to create one?

X: Yes, as a user.

Y: Eh, well, then I would Google some services, I suppose.

X: Oh, I mean the [the professional services firm] VPN.

Y: [the professional services firm] VPN. Eh, I don't think I fully understand your question. To create a [the professional services firm] VPN?

X: Yes-

Y: Because it is already there, right?

X: If you want to connect to the [the professional services firm] VPN-

Y: Yes.

X: What steps do you take to make that connection?

Y: Eh, well, we have this [access token provider] token. It used to be a physical token eh, but now it is an application that we have on our work phones. Eh, and in the bottom right of our laptop we have this connection screen and you can click on [the VPN of the professional services firm]. Then you need to fill in eh, your own passcode, including the token inside this application eh, and then you're logged into the VPN.

X: Okay, and you said it used to be a physical token, is that still an option?

Y: No, no, the physical token I think we stopped using that two years ago. Or longer even.

X: Okay. On what devices do you use the [the professional services firm] VPN?

Y: Eh, only my laptop I suppose.

X: Okay. Do you have an, a phone from [the professional services firm] as well?

Y: Yes.

X: And do you use a VPN on that?

Y: Eh, well, on my phone I don’t need to log onto a separate network, but I do know there are other eh, authentication mechanisms, to still identify that I work at [the professional services firm]. Eh, yeah, I am not sure if you can call those VPNs.

X: Okay. Could you explain to me how a VPN works? If you'd like, you can use the whiteboard for this. I will remove my drawings.

Y: [start drawing 9\_1]. Eh. Well, have my laptop here, and you have internet here. Doesn’t show up. This doesn’t work the best for me, but just gonna leave it. Eh. Draw a straight line. Suppose normal circumstances, you'd have this direct connection from your network to the external, yeah, to the internet, to whatever sources you eh, you might want to visit. [start drawing 9\_2]. And a VPN is, it is like a private network that you connect to using eh, yeah, different kinds of methods, I our it is using the eh, [access token provider] token. And via this VPN you connect to the internet. [start drawing 9\_3]. And then you don’t have this anymore. That's a very simple graph, but yeah, because I am not too technical, I am probably missing a lot, but eh, I think this is how it works.

X: Okay. And could you tell a bit more about the bubble with VPN?

Y: Eh, what would you like to know about it? Like-

X: Well, for example, you said it makes the connection secure-

Y: Right.

X: Is that somehow visible in this drawing?

Y: Eh, well, what is visible already is of course that my personal connection is not linked to the, the external network, that already makes it more secure. Eh, yeah, it also can filter or block out some traffic that is unwanted. [start drawing 9\_4]. So, I don’t know, I can draw a filter in here, maybe, just over there. I guess. Eh, that makes it more secure. Yeah, I am not too creative in this, I expect you notice.

X: No problem.

Y: How can I demonstrate this in this picture. That's a good one.

X: Yes, or any other things that come up related to the VPN.

Y: Eh, no, it masks your identity eh, it filters some data traffic that is unwanted, I guess it is two-way, so there is always an arrow back of course from the internet to the VPN. [start drawing 9\_5]. So, can also draw this, I suppose. Then in here there is also a filter. Eh, yeah, maybe, what else, yeah, something about the location maybe, I don’t think the location makes it more secure, it is just a different location eh-

X: What do you mean with I don’t think the location makes it more secure?

Y: Yeah, so, like my personal network can be here in [place], but the VPN can be a server hosted somewhere else in eh, I don't know, in [place]. It just connecting via different location, such as [place] for example, doesn’t necessarily make the connection more secure. That is what I mean.

X: Okay, and what is a server in this drawing?

Y: Eh, the server, well, the server that my internal server speaks with in order to eh, identify myself and then reroute my data traffic to the external source, to the external party.

X: Okay. And you have drawn two filters, is there a difference between those two?

Y: Sorry? Difference between?

X: A difference between those two filters.

Y: Eh, no, I suppose not. I think, what I have in my mind is just eh, a whitelisting and blacklisting feature eh, so if I am connected to the VPN, they can eh, they can regulate what sources I visit. For example, if the [the professional services firm] network does not want me to use [cloud software] to share files, then they can filter out eh, [cloud software], or even block it. Eh, yeah, it depends what measures they have. It can also have alarming eh, signals that someone who uploads something to [cloud software] that an IT team gets notified or something and then they can take appropriate action, I am not too sure what they do. Eh, yeah, so I guess two level, so one is signaling, they can manage data traffic and secondly, they can actually block websites, which I guess is what I mean here with filtering. So maybe they can block me from visiting [cloud software] website. Eh, and the way around, yeah, the traffic coming in eh, from the internet, maybe when I am downloading something. If they don’t want me downloading a huge trojan from a shady website, then they can block the website, or they can even block the download. Eh, yeah, does that answer your question?

X: Yes, it does.

Y: Hmhm.

X: And if we would change the, your location, so your personal network would change eh, to a location in a coffee bar, would that alter this drawing?

Y: Well, just the location, no. If you consider all the same safety measures eh, no, I don’t think so, the only thing that changes is your IP-address, right.

X: Yes, okay. And then another question. What is the influence of a VPN connection on your computer security?

Y: Eh, difficult question. Yeah, I already mentioned the part about the IP-address, that it eh, yeah, instead of my IP-address talking with the outside world, it is the VPN. Eh, yeah, other than that. No, I am not so sure what I can add, what I already told, told you.

X: Okay-

Y: Maybe my understanding is just too limited.

X: No problem, this is very good already. Eh, what kind of digital threats do you deal with on a normal day?

Y: Digital threats eh, as an [the professional services firm] employee or just a regular internet user?

X: As an [the professional services firm] employee.

Y: Well, I guess we work with a lot of confidential data, you wouldn’t want that leaked. Eh, we're talking about security threats, right?

X: Yes.

Y: Yeah, we, yeah, we wouldn’t want confidential data to be leaked or sent to the wrong party. It can be a lot of sensitive data, that [0:21:20 till 0:21:31 has been omitted]. Yeah, so of course data security and confidentiality is a very big thing for us. Eh, yeah and that's a challenge we face on a day by day basis. Like how do you [0:21:42 till 0:22:04 has been omitted]. Yeah, and storing the data that we have of course, like we often work with [0:22:16 till 0:22:34 has been omitted]. Yeah, that's something that you want to safeguard, of course, offline on your laptop and you don’t want that leaked out if someone were to, for example, gain access to your laptop. And we also work with [0:22:50 till 0:23:21 has been omitted]. So, that's also same thing that you want to safeguard. Yeah, and from myself just to upload all the documents that I have, that I use to [cloud software], yeah, since that is eh, more secure than just having it on my laptop. You cannot just access eh, so the name of that tool is called [an internal page], you cannot just access [an internal page] eh, without the proper access rights. Eh, does that answer your question or are you looking for something else?

X: Yes, that answers the question. You mentioned threats that are eh, like, from a perspective from what you can do wrong or what other employees can do wrong, but are there also threats that come from the outside?

Y: Eh, yeah, I guess, if you download the wrong file, it has a keylogger or something, that someone can steal your passwords. Of course, you have trojan horses, worms eh, yeah, what have you, just, I guess in general viruses that you would not want in your computer that can hinder the data, remove data or even steal data. Eh, that is something that we would not want and that comes from the outside. And yeah, what else, maybe not a security threat, but more from an availability standpoint, you have also DDoS attacks of course. If some party were to perform a DDoS attack on [the professional services firm] eh, to take down the servers, then we cannot work anymore and that's yeah, that's also a threat that we would not want. Eh, what else. Eh, I think those are the main, the main things.

X: Yes, very clear. And how does the threat change because of the VPN connection?

Y: Eh, like I said, so, they can, of course you can acquire viruses through different means, like it can be eh, through a USB stick for example, it can be because you download a random file from the internet. Eh, I think a VPN can eh, manage that. If you'd log onto a network, they can eh, like I mentioned before, you have this filtering or at least these signaling controls he, where, where the managers of the VPN they can identify it and they can block it. Eh, to prevent these things from happening. For example, if I bring in a random USB stick, they can identify that and even stop me from using a USB stick. Eh, or they can prevent me from visiting a malicious website, or downloading malicious software. Eh, I think a VPN can play a big role in that.

X: Eh, and do you also mean that a VPN eh, would be able to stop you using a USB stick?

Y: Well, of course, I can plug it in myself, eh, but for example, what files can be run, like if it has an alter executable on the USB stick, I think a VPN can play a role in that, in preventing, or at least detecting what I am doing, with the data on the USB stick.

X: Okay. And you also said that it can eh, block certain things coming to you from the internet-

Y: Hmhm.

X: What kind of things could be blocked?

Y: Eh, just websites, I suppose. If they know that eh, www.virus.com is eh, is a malicious website, they can block it. Then I cannot visit that website. Is that what you mean, or?

X: Yes. And is a VPN able to block any other things as well?

Y: Eh, well, websites, download, yeah, I guess it regulates data, if you put it broadly.

X: Yes, okay. Eh, and then also, this was about digital threats-

Y: Hmhm.

X: What kind of social threats do you deal with on a normal day?

Y: Social threats. Can you define social threats?

X: Yes, I mean all threats that are non-digital.

Y: Very broad description. Eh, difficult question. Let me think about that. You are still talking in the area security, right?

X: Yes.

Y: Eh, your question is does a VPN help with that, or does it block those threats?

X: Well first of all eh, it is more in a general sense-

Y: Hmhm.

X: So, what social threats do you encounter on a normal day, if you don’t take the VPN into account?

Y: Well, eh, maybe to take your coffee shop as an example or coffee place, eh. If [0:29:14 till 0:29:16 has been omitted] and then I want to, yeah, maybe work from a [example of restaurant], you often have eh, an open network, like everyone can sign on to it, but that also means that eh, well, it is an unsecure connection to that network. Eh, not sure where I am going with this, but eh, let's say I am working there and eh, I don't want someone looking on my screen or something and then someone else is sitting behind me and can look on my screen. Then I guess that is a social threat and having a VPN does not help with that. Eh, yeah, what else can I really think of.

X: You shortly mentioned an open network-

Y: Yes.

X: Eh, does that eh, matter for the VPN connection? Or would that pose a certain threat?

Y: Eh, I think not for the VPN maybe, but it could be a threat for my own laptop, I suppose.

X: And how could it form a threat?

Y: Eh, from, from what I read, I am not too sure how accurate this is. Eh, if you'd just connect to an open network, especially if it is unencrypted and you then use your laptop and you log onto websites, eh, fill in your credentials, then this open network, or the person who operates it, or the group. Eh, they can actually view what, what data I am sending. So, also what my username or password was if I, if I fill that in. Eh, and then this other threat is of course someone is impersonating that network and then someone eh, hosts a private, sorry, an open server on his phone or laptop and impersonates that he is [example of restaurant] and I log onto that network and I give my data or I sign onto websites that I normally use, then, and then my data could potentially be stolen. I think that's eh, that’s a possibility. It never happened to me. Eh, yeah, does that help?

X: Yes, it does-

Y: Or are you still looking for something else?

X: And how does the social threat change because of the VPN connection?

Y: Eh, I don’t think it does change. I’m thinking what other social threats are there. Like social threats if eh, the social threats impact people. And people are always I think the weakest link in security. So, if someone eh, approaches me and can look onto my screen, if I have confidential data on my screen and someone looks at it, the VPN does nothing for that. Eh, there are some physical measures that you need to take, like eh, eh, I don’t know how you call it, but like a screen so someone else cannot peek onto your screen. Eh, yeah, well, what else. If someone impersonates that he is my boss for some reason, eh, he is my boss and needs my password, and I give it to him for some reason, I guess that is also a social threat. Then, yeah, having a VPN also does not help for that of course. Eh, yeah-

X: Yes, and the other threats you mentioned, of using an open network, does the VPN have a role in this?

Y: Eh, yeah, I guess, eh, yeah, because then the VPN still replaces my own network, I suppose. Eh, and that, so, the VPN can still regulate what data I send or eh, or that gets send, so in that sense I suppose if I log onto a [example of restaurant] network and then my VPN, then my connection would be more secure, yes.

X: Okay. And If you think about these digital and social threats, who or what could be an attacker behind the threat?

Y: An attacker. Eh, you need to split it up. So, digital threats, so, I mentioned viruses, that doesn’t necessarily have to be a person, eh, ...(0:34:29), but you yourself are the threat basically, because you would need to be the one to get it in. Eh, yeah, if an external person were to try and brute force my login code and password from an external source, I guess that's also a possibility, eh. Can you repeat your question again, eh-

X: Yes.

Y: For the social part.

X: The question is who or what could be an attacker behind the threat.

Y: Hm. Who or what, eh? Yeah, like a hacker or a person can eh, try and brute force into my server, I guess a person is a hacker, it can be anyone with malicious intent. What, it can be a server, a server hosting a website with malicious data, that if I were to visit it and download it, that is a threat to me. So, I guess a server-

X: Okay, and if we look more into the persons eh, could you give an example of a person who would be an attacker or could be an attacker?

Y: Eh, so again, me as a [the professional services firm] employee, right?

X: Yes-

Y: Who would want to attack me. It is a difficult question, I don’t see a reason why they would want to attack me. Because then they would first need to know [0:36:33 till 0:36:35 has been omitted], what confidential data I have, before they would want to even specifically target me, eh. So, it is very hard for me to give an example. Who would want that?

X: Okay, and if we look at a more abstract level to [the professional services firm] as an organization as the target.

Y: Right, yeah.

X: Then who or what could be an attacker behind a threat?

Y: Eh, I guess two main things that people would want to steal I guess are the personal data of all the [the professional services firm] employees, the names, addresses, yeah, just all personal data, cause that's valuable to them. You can sell it off to what have you. And of course, we have client data, those are the crown jewels I suppose of [the professional services firm]. So, if anyone were to want that, eh. Yeah, personal data is anyone who is after quick money, I suppose. Eh, yeah, I still call them hackers, cause I just don’t have a better term. It can be anyone. Eh, yeah, and for client information, yeah, same for that, but maybe, because we are thinking more about [0:38:03 till 0:38:09 has been omitted]. But then again, it- The same term applies, it is still hackers. Eh, yeah, I don’t think I can really specifically name a person or a group of people who would want to perform this.

X: Okay. And what would be an attacker’s capability?

Y: An attacker’s capability. Eh, what do you mean by that?

X: Eh, what would be an attacker’s background need to be to be able to perform an attack?

Y: Depends how sophisticated that attack would be. Eh, Yeah, there are very, there are a lot of ways to attack, so to say. Eh, if it is just setting up a malicious website, then I suppose you need basic knowledge of how to set-up a website. Eh, if you want to program your own eh, virus, your own trojan, then I guess you also need some coding experience. Eh, I don’t think there is a study to become a hacker. Eh, yeah maybe, you have ethical hackers of course, but yeah, suppose then, yeah, just some programming background would help of course. Eh, yeah, but there is plenty of information online of course. Like if you want to become a hacker eh, you can do it. You just need eh, to know where to find it on the internet to get the right eh, coding knowledge and then you need the experience. Just need to try it.

X: Okay, and how does the kind of attacker change because of the VPN connection?

Y: Eh, yeah, eh, I guess a potential attacker can also be someone already working internally at [the professional services firm]. So then, yeah, if you don’t have access to the VPN, then you cannot be eh, an internal employee. And if you do use an employee eh, if you do use a VPN, then the attacker could be an internal employee, who already has access to the network. I guess that is a change. Other than that, I cannot think of anything else.

X: Okay. And if we think from the perspective of [the professional services firm], what could be the impact of an attack?

Y: Phoe, huge, I suppose. Eh, first as personal data and eh, the biggest thing is of course the confidential data, if we lose our client data eh, yeah, that is a major breach in trust. Eh, our clients trust us with their confidential data, and trust us that we safeguard their data. If we lose that it is just a lot of reputation and eh, brand damage to [the professional services firm]. [0:41:35 till 0:41:40 has been omitted. Our entire practice is based on trust, without trust there is no [the professional services firm]. So, in that aspect, yeah, it would be catastrophic to [the professional services firm] I think if that happens.

X: Can you think of any other impact?

Y: Eh, other type of impact or eh, what do you mean?

X: Yes, other type of impact.

Y: Eh, yeah, it can have financial impact, I suppose. Like it would cost a lot of money to eh, find out where the leak happened and to close this leak and to track all the data that you lost and follow up with the client as well, because of course you need to report this to the local authorities, to the AP for example. And eh, most definitely to the client, you need to report it to them, that you lost their data, eh. [0:42:38 till 0:42:39 has been omitted]. The client needs and has the right to know that their data has been compromised as well. So, you need to communicate that. [0:42:45 till 0:42:52 has been omitted]. Eh, yeah, so a lot of time, and effort, money is involved as well, I guess, that is also a major threat. Eh, is that what you're looking for, or?

X: Yes, it is.

Y: Okay.

X: And now another question. Eh, if we look at the VPN connection itself-

Y: Yeah.

X: How secure is a VPN connection?

Y: How secure, I don’t think I can answer that, it depends. It depends on the operator of the VPN, how secure the person or the group makes it, right?

X: And what would you mean with how secure it makes it? What could change?

Y: Eh, the filters that they apply. If I log onto VPN, what filters do they apply on data traffic or what, what data traffic do they block, that is something that the, the operators of the VPN can configure. Eh, if they don’t configure it, then it is maybe not very secure. If they do configure it and go very far, like even block my [e-mail] use, that I don’t send some confidential data to my private email or something, it can be very secure, but also very annoying for the users. So, yeah, my answer is, it depends.

X: Yes, okay, very clear. These were so far my questions. Is there anything important to know about VPN that I did not ask about?

Y: No, I think you did a good job. You eh, well, at least my knowledge of VPN is very limited, so, I think you asked- You pulled all the knowledge out of me about VPN, so in that case, yeah, good job.