# Transcription expert 4

Duration: 88 minutes

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

Y: A VPN is used to reroute your connection through the server. Eh, this is used for security purposes or to eh, be able to mask your eh, location while using the internet.

X: Okay. You say to reroute your connection, how is your connection rerouted?

Y: So, you are using it as a door to the internet instead of connecting to the internet through eh, your eh, connection, your IP, your computer you are accessing this server and from that server you are sending your requests and receiving your data and then it is routed from the server to your computer.

X: Okay. And could you explain to me what a server is?

Y: Eh, basically a server is just another computer that you're connecting to. A server is of course eh, bigger, stronger computer, this is eh, eh, let's say industrial or something. This is a computer that is eh, eh, used for multiple users. This is a mainframe like a, as you can see in the movies eh, a cabinet closet, that eh, has the, the, eh, supercomputer, the stronger computer than normal. And you are using it as a connection. You are connecting to it and the server itself, that computer itself is sending and receiving requests from all over the internet.

X: Okay. And you said you can use VPN for security purposes, could you say more about what these security purposes entail?

Y: Eh, so, eh, you can think of it again as a computer. In your computer, you have your own eh, antivirus computer eh, software, you have your own malware, you have your own eh, eh, security applications all of those are eh, eh, embedded within the server with the highest level and with the eh, latest updates. So, from eh, eh, the threat of being eh, infected with viruses, breaches, or eh, being hacked, using VPN is an extra layer to eh, safe, to make you a bit safer than searching the internet. So, when you are accessing a website eh, which is eh, suspicious or eh, that can eh, trigger a virus, this server, this VPN server, can act as a first layer of, of eh, of, of defense. So, this is one. The second one is security from the eyes of everyone else. So, from the people who are tracking your requests, tracking your eh, eh, browsing history let's say. While using VPN, no one can see what are the request that you are sending, they can only see the IP of the server itself. So, you are also shielded from being tracked.

X: Okay. And your first security purpose, how does the server act as a first layer of defense?

Y: Imagine that eh, this server is eh, your PC. And you are connected to this PC. Imagine that it is in your home, in your room, so this server eh, has the latest version and the strongest version of antivirus, it has the strongest version of anti-hacking or malware, as they call it. So, the malware is software that people can use to eh, obtain information from your laptop or your computer. So, using this server can provide this extra layer whenever there is virus that is coming to your eh, browser, coming to your PC, coming to your laptop. Through this server, the server should act as a, a, firewall, a defense layer, that's stopping this virus. So, eh, yeah, for example when using a VPN, sometimes you are trying to access a website and you will not be eh, directed to the website, instead you will get a screen that this website that you have requested is not secure, using this connection you will not be able to access this website. Eh, we recommend you to look into eh, eh, this website as it is reported as a threat to your PC. So, it either stops you from entering the website, or stops the intended threat, so it can stop the attachment or stops an e-mail from coming to you if it is eh, eh, including any threat to your data or to yourself, your PC.

X: Okay. And eh, you also said it protects you against the eyes of everyone else-

Y: Hmhm.

X: How does this protect you against the eyes of everyone else?

Y: Okay. I'll give an example eh, outside of our environment. Then I'll give another example from, from work perspective. So, from eh, countries that are at war, for example [country], is someone who can speak against eh, eh, a certain party. There is a possibility for them to be detained or eh, held accountable to what they are saying. So those people use the VPN and through the VPN they can post, they can send files, they can use accounts, without these parties being able to track them or to know who is the actual person responsible for those information. The VPN, using the IP of the VPN, everyone else on the internet is they can track an account or an article or a video on [social media platform], they can track the IP that has posted this. And this IP is one of the IPs of the server itself, of the VPN server, but if the VPN is secure, which is, should be the case, you cannot get the IPs of the people using this server, you can only see the actual IP of the server itself, not for the users who are using this, this server. So, this is one of the uses of masking your own IP. Hiding it through the use of the VPN server. Is this clear?

X: This is clear. Thank you.

Y: Of course, another application from, from work perspective eh, when you are working with eh, multiple clients and international clients, sometimes there are some limitations to accessing their data. [0:09:25 till 0:09:36 has been omitted]. And I can only access this information if I have an account that can allows me to do that. So, using the VPN connection masks my ID, of course this is in a legal way, I mask my ID through their VPN, so that I can access their secure eh, location. Using this VPN can give them the comfort that I am not an intruder or someone who is not authorized if I have this VPN access it means I have the permission to go to their secure eh, cloud, and access their files.

X: Could you perhaps use the whiteboard to draw for me how such a connection would work? You are for example working from your home situation and you connect to eh, [the VPN of the professional services firm].

Y: Eh, I, I don't know how to create this eh, let me try to see if I can eh, interpret this in a simple way. [start drawing 4\_1]. So, instead of connecting to the internet immediately, we can use the server, let's use this IP. This is my PC. This is the VPN. And this is the eh, internet or if we can say the, o, wrong button. [start drawing 4\_2]. O, let's quickly draw it eh, this is [the professional services firm], this is the VPN. Eh. Normally I would connect to [the professional services firm] using my IP, which is my internet name. [example IP-address], so the IP is the name of my connection, you can consider it the name of my eh, eh laptop. The internet knows me as, as this number. So, when I go to [the professional services firm], [the professional services firm] sees me as this and it will not allow me to enter this, their server, to access their services. For example, to go into my e-mail account, my [the professional services firm] e-mail account. Eh, or my eh, eh, work eh, workspace. So, I need to have a secure connection because this can be copied easily, this is a public IP, so anyone can use this public IP. Of course, I can combine this with a password or with another authenticator, but it still is eh, a bit eh, vulnerable. So, people can hack or can eh, use this, another combination to hack my account. [start drawing 4\_3]. So, [the professional services firm], they have installed another layer, this layer, means that access from outside is eh, access from outside is not allowed eh, unless it is secured. [start drawing 4\_4]. So, how can we make this secured connection is to have eh, for example a number of secure eh, IPs, let's consider [example IP-address] until [example IP-address]. Yeah. So, this is an example. Of course, it is a bit more complicated than this, but this is the concept that they have private IPs that are only known between the server and [the professional services firm]. [start drawing 4\_5]. Then, if I want a secure connection I can connect to the VPN, using my IP-address. Using this address. And then from the VPN, when I connect to [the professional services firm], I would use one of those secure eh, IPs. [start drawing 4\_6]. So, [example IP-address] for example. So, [the professional services firm] can only see this IP and because it is an IP that is eh, in their database they can allow it to enter. So here in the database, [the professional services firm] should have the list of those secure IPs. So, [example IP-address], for example. So they are saved here, so, they crosscheck those IPs with their list, and eh, this is the eh, let's say the contract between this VPN and [the professional services firm] to allow those IPs and then I can enter their eh, secure application and eh, do the work. Is that eh, good, is it okay.

X: Yes, very clear. You told earlier about a firewall as well-

Y: Hmhm.

X: Where in this picture would you find a firewall?

Y: So, here, within the VPN, now I send my request, now let's consider another scenario, where here, instead of [the professional services firm] I am visiting unknown website. So, if I am, let's say eh, using instead of [the professional services firm], am logging to on unknown. [start drawing 4\_7]. Let's call it- So if I want to go to this website, I send the request with a secure eh, IP. [start drawing 4\_8]. This website sends back eh, a packet data, a picture for example or a sort of data, that has a virus in it. Let's say virus, a virus here. So, this is a virus. [start drawing 4\_9]. Now, within the VPN, they have the applications that should eh, scan all coming packages eh, and for example, anti-virus, anti-ware, eh, firewall- So, all of this is within the VPN, so the server, this computer, is equipped with all of the state-of-the-art applications that scan those packages and either remove eh, here, either stop, eh, wait- [start drawing 4\_10]. Either stop this here, at this border, or for example only allow the secure part of the package and will not, so for example you are receiving an e-mail from an unknown source, you will get the e-mail, but you will not be able to open the attachment. So, the attachment is deactivated for example. So, using the, the software is within the server, you eh, make sure you have a more secure connection with only eh, known eh, sources or known objects to be received. Is that clear?

X: Yes. You also said-

Y: So, it is-

X: Yes, sorry.

Y: Yeah, so, it is similar to what you could have on your own eh, device, so for example you are using eh, eh, some kind of an anti-virus, [software provider] eh, [software provider] anti-virus. But what you have on your PC, you have the personal version, because if you want to have the corporate version, you will need to pay a lot of money. So, this company, the one that has the VPN server, they pay for the highest level of security so that you are using this very expensive and up-to-date application for, for your personal use. So, you are using the technology with only fraction of the cost.

X: Do you need to pay yourself you mean, or the company pays it for you?

Y: Exactly. So, if you want to for example, if you want to install five applications, if you want to install one application for antivirus, if you want to install one application for secure browsing, if you want to install an application for anti-malware, eh, if you want to install eh, a firewall, so, in the end you will need to pay for example a hundred euro per month, but the VPN pays a thousand per month, because they have the updated version, the up-to-grade version and then they only ask you, or they ask your company, for example in my situation [the professional services firm], they ask for ten euros per user, so they get back their investment and the user herself, the user himself, doesn't really pay for the total cost of the application, they only pay for the monthly subscription to the VPN itself and use the software.

X: Okay. And you also mentioned that sometimes a page, a webpage is unsafe, and your browser blocks it. What is-

Y: So, it is the same, it is the same, sorry, it is the same with this if you are going to an unsafe eh, website, it doesn’t wait until you get back the virus and stop it, the VPN has also a list eh, let's say here. [start drawing 4\_11]. So, it could have a list of secure websites, or a list of unsecure websites. So, the VPN server, they have a list and they compare every request. So, every time you type www.google.com for example, this request goes through this filter, the filter looks if this is one of the secure websites, it immediately allows it to go, if it is one of the list of the unsecure websites, it immediately stops this request and sends it back to you and inform you that this is not secure, because this has been reported for example earlier. So, your request is not send or the third option is your request is not being recorded on either list, then the eh, request is send and then the response will be eh, eh, scanned for any viruses or any attacks, and then it's stopped if it is the case.

X: Okay. And what would happen if you go to the same website, but you are not, eh, you did not enable a VPN?

Y: So, now, if you are bypassing this, if you are going immediately through the normal connection, then your request will get to the website and the website have the ability to send you eh, a virus or spyware or malware, and it is up to your device, laptop or PC, to stop this attack. So, do you have up-to-date antivirus, do you have an up-to-date spyware, then it will catch this eh, this attack. If it doesn't have it, you will receive it, for example an e-mail with an attachment, an e-mail with a link that can install a virus. So, the laptop or the computer didn't catch this attack and you received the e-mail, than it is up to you to open this e-mail and see okay, I see this e-mail, it doesn’t look phishy, I click on the link and then I am eh, infected, my laptop is infected with a virus. But then, the other option is I notice this is an attack, I notice this is not secure e-mail and I delete it. So, if I am not using the VPN, I am depending 100% on my eh, self and my device.

X: So, there is no other mechanism that prevents eh, e-mails like that being send to you?

Y: [start drawing 4\_12]. So, as I said, the mechanism is either one eh, let's say, VPN or paid apps or free apps and then your knowledge and eh, eh, your knowledge and eh, let's say, common knowledge more or less. Eh, so eh, the most secure option is to use a VPN. The second option is to pay yourself for the applications that the VPN is using, sometimes it is not at the same level, but a paid eh, antispyware or antivirus is also an option, if not, you can install a free version. So, this is partially protecting your PC. Of course, it is not protecting it from eh, from the latest eh, applications. Because the latest ones are always covered by the paid version. If you don't rely on those free apps, then you are relying on your knowledge. So eh, last month, I received eh, an e-mail from my account from [e-mail], asking that eh, there is an attack and you need to click on the link to change your password. I immediately saw that this e-mail is not from [e-mail], it is an attack that looks like a [e-mail] page, but if you focus on the eh, e-mail that this e-mail was send from, this is eh, not @[e-mail].com, but eh, gibberish, something else. So, when I saw this e-mail, I understood that this is an attack and I e-mailed immediately reported this e-mail instead of opening the link. Instead if I had opened the link and I got to a website asking me write down your old password and new password, they would get my old password and they will open my account and get inside my account. And eh, eh, get my information. So, eh, the VPN is the most secure way to browse the internet, but it is not the only option, it is the most secure option.

X: This is for your corporate laptop?

Y: I am now talking in general, either for corporate or eh, personal laptop, but this is a good question, because within a VPN you have multiple eh, types of VPN. So, you have the commercial VPN, some company who bought a server, put it online and ask people to pay subscriptions to use this VPN server. So, this would be secure, but it would not be highly secure. Then you have an, another VPN server which is from a well-known corporate, so for example using secure [company] server. So, this [company] server, they have a name they need to maintain so they use a really state-of-the-art server. So, this is the second level. The third level, which is the highest level, is that a VPN that is provided from your corporate, from eh, for example from, where I work at [the professional services firm], they have provide their own eh, VPN, this is known, this is the highest level. Because, then here, you are not using the IP from the VPN, you are using a VPN that is pre-approved by the company, so you have two-way handshake as they call it. So, the VPN communicates to [the professional services firm], and [the professional services firm] communicate to the VPN and they open a secure connection. So, this is the highest eh, the highest level. There is no way of anyone intervening in the middle. No third party.

X: What do you mean with interfering by a third party?

Y: Eh, the VPN company for example. So, the VPN company, if you look at the internet, there is a lot of eh, eh, third parties, there is a lot of companies who eh, yeah, sell you the service of VPN. But are they themselves secure, you don't know them. You need to do your own research to make sure that those companies add service are secure. They have the latest update of the antivirus and they have a good secure connection. Because sometimes a VPN does not mask your ID, the IP-address. It allows your IP-address to go through, but it scans the package. This is not a hundred percent secure. But if you are using a VPN that is pre-approved with the websites that you are visiting, then it makes it, eh, another layer of security.

X: Okay. Clear.

Y: Okay, good.

X: What do you mean with a secure connection between the VPN server and [the professional services firm]?

Y: So, the, what I mean by secure connection is what I just mentioned. So, the secure connection is that no one else is between you and your target application. So, if this VPN is provided by [the professional services firm], so you have immediately from connecting from your PC, you have [the professional services firm] channel. So, I don’t have any other company that could be a weak link. So, I have a secure pass. So, for example now in this pandemic, in Corona. So, I have, I go from my home to my car, to my office. Which is, I am the only one who is using this office, so I know all of the steps that secure, no one could eh, infect me with this disease. But, if instead of using my car, I am using public transport, there is, here, this connection in between, is not secure. I am not using an eh, corporate VPN, I am using an open connection. So, there is a big change of being infected if I myself, not being vigilant, I don't have the knowledge of protecting myself. Of course, instead of going in the public transport, I can use eh, my neighbor’s car, my brother's car, I can use a taxi company. It is eh, less public, but again I don't have the 100% assurance that this is eh, risk free. So, using a VPN is like using your own service. You know how secure it is. But using any other option car present more risk.

X: You mean you know how secure the [the professional services firm] VPN is.

Y: Eh, of course, in this situation it is not me who need to be afraid, it is [the professional services firm] who needs to be afraid. And they know that this VPN is secure. Me, as a user, I don't know. But because [the professional services firm], who is the, let's say the organization or the site that need to secure their files, they are the people who eh, take the measures to make sure that this VPN provider is secure. And they do that by, for example, a strong contract with eh, a penalty clause, if there is any eh, issues eh, with doing an audit. So, the IT-audit itself is one of the ways to make sure that the eh, service that is provided is according to the standard that it is mentioned.

X: So, [the professional services firm] uses an external VPN supplier you mean?

Y: Eh, so [the professional services firm] is using a VPN supplier. I cannot eh, I don't have the knowledge if this eh, for example a company or an application owned by [the professional services firm] or this a contract being eh, extended by, with a third party. The only thing is, I know that, the [the professional services firm] VPN is a service eh, like [the professional services firm] e-mail address. This is service that is provided by [the professional services firm] to its employees and it is managed and overseen by the corporate itself.

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

Y: Eh, so, the VPN itself is only used on eh, [the professional services firm] laptops. But of course, there is other measures on other devices. So, if you are using your mobile phone to access [the professional services firm] location, you need to have another service. Not a VPN, but a service that eh, checks for eh, your connection and your requests. So, it is not a VPN, but some sort of eh, check, like an antivirus for example. It is not an antivirus, but it is eh, a service to check for, for threats.

X: Eh, why do you use a VPN? For what purposes?

Y: The purposes of using a VPN. Is that your question?

X: Yes.

Y: So, as a [the professional services firm] employee, I use VPN to eh, first of all, have a secure connection eh, to, eh, to have the eh, I'm trying to find the right word. So, eh, to, provide my clients with the assurance that their data, which I am working on, is still secure. So, no one from outside my organization, my team can have access to their data, which is on my devices. So, using a VPN eh, provides the assurance that the client data is secure.

X: Are there any other purposes for which you use a VPN?

Y: Eh, for my personal use I could use a VPN for example to access the [company] server on the UK, because the server on the UK provides broader content than the content on the Netherlands, but- And of course, I am stating this a legal way of using the VPN. Other people can mask their eh, their, their IP to eh, access eh, other websites that can track their eh, usage of the VPN. So we are going back to the first question eh, the usage of the VPN is either to mask your presence, your name, your IP form anyone else on the internet or to have a secure connection to be able to access any website without being afraid of being hacked or eh, having a virus on your device. Eh, or to have a secure connection with no one else being able to steal your data.

X: Do you mean no one else can steal your data because you use the VPN of [the professional services firm] and not another VPN server?

Y: Because I used a secure VPN, not an unverified VPN. Because other VPN services could be secure, but again, here in my situation, [the professional services firm] did the work for me. So, [the professional services firm] have provided the assurance that this is a trusted service. I don't need to do the work myself. But with other services, I do need to do my research, I need to review the contract, which 99.9% of the people don’t review. So, when you are subscribing to any contract, you get approve and do not approve, most people press on approve without even reading what they are approving on. So, this is something that, when I am using the VPN of [the professional services firm], I know for a fact that [the professional services firm] has the legal team to make sure that eh, using this service has been reviewed and eh, approved by the company.

X: And as a user, what actions do you take to create a VPN connection?

Y: Eh, as a user, I only open the application that is provided by [the professional services firm]. I make sure that I have the internet connection activated. I put my username and password a click on connect.

X: Okay. And what is the influence of a VPN connection on your computer security?

Y: [start drawing 4\_13]. If the VPN connection is on, I know for a fact that here I have this connection protected. So, whenever the VPN connection is on, I know for a fact that I won’t, most of the time, I won’t get any threats from this side. [start drawing 4\_14]. The only problem is that when I turn off my VPN connection, I could get a risk or a threat from this side. [start drawing 4\_15]. And if I use a, a USB for example, a USB stick, in my device, this is a threat that the VPN is not covering. So, the VPN is only covering the risks from the internet, as long as the VPN is activated.

X: Okay. And does it matter where you create the VPN connection?

Y: Sorry?

X: Does it matter where you create a VPN connection, so for example at home or at a different location?

Y: No. It doesn't matter, because, no matter where I am, immediately when I am activating my VPN, I am doing this two-way handshake. So, I am sending a packet to the VPN server and the VPN server approves my connection. When it approves my connection, this connection is encrypted, so no one can access this connection, and this connection is protected by eh, the VPN server itself. I don't know if you can see my mouse when I am moving it.

X: Yes, I can. Can you tell a bit more about the encryption of the connection?

Y: Eh, this is another layer of protection. So, a VPN could provide encryption. This encryption means that like when we are talking in a different language, the VPN is using another language. So the letter, or the number one in the eh, computer language is eh, sevens zero's and a one, so it's eh, in the computer language, in the language of zero one, eh, number one is zero, zero, zero, zero, zero, zero, zero, one. With an encryption eh, the VPN could be using a different language, which eh, cannot be read by an outsider who doesn’t have this eh, list of decoding of the encryption. So, using the encryption, the information is sent and received between me and the VPN server in a way that is not being read by anyone else. Even if they were able to tap into this connection.

X: The connection between the VPN server and the [the professional services firm] server?

Y: Between the VPN server and [the professional services firm] if this is like for example in this case, this connection is a private connection, then I would expect that here, there is also an encryption. The encryption only works if the two parties are eh, known to each other. So, they have the let’s say, decoding list. So, if I speak to you in Spanish, and you don’t know, you don’t have the dictionary of Spanish, you cannot understand me. But in this case, all of the parties have the contract, so they could have the decryption list, therefore I would expect that all of this connection is being encrypted.

X: Clear, thank you. And then in a bit of a broader sense, what kind of digital threats do you deal with on a normal day?

Y: Sorry, I did not get the question.

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

Y: Eh, may I ask you, can we take a break for eh, couple of minutes?

X: Sure.

Y: Okay, I will keep the connection on, I'll just eh, come back within three-four minutes.

X: Okay, that's fine.

Y: Okay.

[break from 0:54:01 till 0:58:25]

Y: Hello.

X: Hi.

Y: Hi, I'm back.

X: Are you ready to take on where we left of?

Y: Yes. Yes. So, your question was, was what are the type of threats that I am facing in my work, right?

X: What kind of digital threats do you deal with on a normal day.

Y: Okay. So, the first threat is that we are working with, with the high-profile clients, so there are a lot of people who would like to obtain this kind of information from any way and they could try to obtain this from, from our laptop or our connection or our devices. So, the first threat is people trying to hack and steal the data of the clients. Eh, the second, eh, level, the second type of threat is the people who would eh, try to steal eh, any data without any discrimination. So, any type of data to eh, blackmail and ask for ransom, eh ask for money. So, it doesn’t really make any, any difference if the data is personal for the client or the organization itself. And of course, the third eh, the third party, the third threat is people who would like to harm eh, eh [the professional services firm] as an organization. So, those three threats that eh, eh, we could deal with eh, using, yeah, digital connection.

X: And how would information be obtained from your laptop?

Y: Eh, by one of the eh, ways eh, eh, shown here in this drawing. So, either by sending eh, spyware and malware, where eh, unknowingly I am opening a connection with this person or this organization and they could steal from my laptop without me knowing. So, they install this application that open this connection. Or by me thinking that I am uploading the files to [the professional services firm], but in fact I am uploading it to a different location. So, eh, as I said before, an e-mail with a link that I think it leads me to a certain website, but in fact it's leading me to a different one. Eh, what else. Eh, sometimes it could be eh, with infecting a computer with a virus that you cannot eh, deactivate until they, you pay this person a certain amount of money, so that he can activate, deactivate it for you, so this is the ransomware. It happened with eh, unknown virus where the data on, on the computer were held hostage, so you cannot access your own data until you eh, had to pay eh, certain amount of money to the hacker, so that he can eh, deactivate the eh, virus and you can access your data. And if you don't eh, some viruses keep your files locked, some viruses delete your files and some viruses even, cause your device to malfunction. Sometimes stop the fan in the laptop to stop, heating the laptop, which destroys the hardware itself.

X: Okay. And you also said that information can be obtained from the connection. How would that be?

Y: Sorry, I didn't get the question.

X: Yes, you also said that information can be obtained from the connection. How would that be?

Y: Eh, the information can be obtained from eh, like, masking the connection, so it's not from, from just listening to the connection itself, but from eh, being in the middle. So, instead of eh, visiting the service or the website that you are thinking you are going to, eh, you are using fake eh, a fake website. This website is being created eh, more or less like a VPN, used to show you what you want to see, but in fact you are not getting to your connection. You are getting to your, a fake, yeah, a fake website in the middle.

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

Y: How, sorry?

X: How does the threat change because of the VPN connection?

Y: Eh, I don't understand the, the connection.

X: Okay. You mentioned there could be a fake website-

Y: Hmhm.

X: Does the VPN connection influence that threat?

Y: Yes. So, the VPN does not stop your connection. It only makes sure that you are as secure as possible. [start drawing 4\_16]. So, if this website that, the fake website that is created, eh, if this is a new website, and it doesn’t have any eh, eh, any eh, people eh, how to say, reporting it. So, no one has reported this website yet, and you have requested an access to this specific website, eh, the VPN search it list, it doesn't find anything, so it makes the connection to this website. If the website is not sending any eh, suspicious files, then the VPN eh, is making this connection. So, the VPN is only stopping eh, suspicious links and suspicious packages, but this is not a common threat, then the VPN is not stopping it. So, the VPN is not 100% eh, risk proof, but it is the most secure way. So, coming back to your question, how, if I have this website, if I am using a VPN, most likely, this request will be stopped here after being checked against the list that are within the VPN. So, if this request if being checked, stopped here, if it is not sent, the request is sent, but getting any suspicious information back, it will be stopped here, and it will not be sent back to the PC.

X: And you say the VPN connection for the VPN server is not 100% secure, what do you mean with that?

Y: Eh, so, one thing that I have learned when I started working on eh, computers, is that if someone wants to hack you, he will be able to hack you. The only thing that you can do is to make his job harder. So, you can install more applications, more, more layers, you can use advanced, more advanced technologies, but in the end if the hacker is experienced and determined to get the information, they will be able to. Eh, the only thing is that you are making it harder and more expensive and more dangerous for the hacker to do so. Eh, so this is for example the difference between using eh, public VPN versus using the corporate VPN. So, if I am using the corporate VPN, I am having a higher level of security. But there is a lot of eh, situations that companies have used secure connections and eh, non the less, there was an attack on them. Of course, the attacks will be less, the losses will be less, but in the end, the VPN cannot stop everything. As I just said, this is one clear example, if this website is created new, there is no report, so this website is not used on any of the lists here. So, my request will be sent. If I have sent in this request any private information, this private information is already known to the hacker. So, there is always a risk and that's why I said the VPN is not the only layer of protection, you need to have your own knowledge and common sense to stop any phishing e-mail, any eh, virus that could be eh, uploaded to your device.

X: Can you think of any other reasons why a VPN is not secure or not 100% secure?

Y: Eh, no. I believe the, yeah, this, this could be the, the eh, the biggest reason. Just that, just the fact that any smart person who put some eh, defensive measures, there is a smarter person who can defeat those measures. The only way to be 100% secure is not to have an internet connection. And that's what some of the companies do, they always have servers that are not connected to the internet. They have their private information on those servers, and keep them offline.

X: You mentioned that there are always smarter persons than you, who or what could be those smarter persons?

Y: Eh, yeah, anyone. So, eh, when I started eh, working in my eh, profession, I had little information, I gained my experience because I have the eh, passion, I have the drive to do so, and I have done the courses, I have obtained the knowledge, I have developed my eh, eh, experience. So, that now I am way better than I was five years ago. The same way goes for hackers. So, there are people who are fully dedicated to break those types of walls. So, no matter how secure and sophisticated, there will be people who are, whose sole purpose is to break those type of eh, secure measures and they are eh, most times succeeding. But of course, the race is that the antivirus companies, the VPN companies, that they are immediately adapting and eh, eh, updating their eh, measures, so that this door is not open for eh, a long time.

X: Could you think of examples of attackers? What kind of categories do we need to think of?

Y: So, one of the most common attackers, known to, to eh, a lot of people are the people who eh, hack the iPhones, of course I am talking about personal use, not the corporate use. So, eh, there are people who break the eh, eh, let's say the, the seal of the company and they call it a jailbreak. A jailbreak is a way of hacking the eh, the iPhone software, so you can install eh, a non-approved applications on the iPhone. So, those people, no matter how many updates the eh, the iPhone company, Apple, is providing for the iPhone, immediately after one week or one month, the hackers are able to break the code and provide an update for this jailbreak. So, this is a clear eh, example of, because there is a need, cause there are people who always want to have eh, unauthorized applications into their iPhones, there are always people who are willing to put the effort to break this eh, code.

X: And does the kind of attacker change because you use a VPN connection?

Y: No, because now, what I am talking about is hacking eh, certain software, this is not related to a VPN connection. But if we are talking to, about hackers that want to hack a connection, or want to hack eh, location, a virtual or physical location, they want to get into your hard drive, then yes. A VPN is one of the best eh, best eh, measures to stop this hacker. Because the hacker here, he doesn’t need to eh, break a code, he doesn’t need to solve an equation. [start drawing 4\_17]. He only wants to find a way, a small way, a small door, so that he can access and get inside the VPN or get inside your device, within, through the VPN or outside the VPN. So, eh, this VPN, if it is strong, if it is secure, it is preventing 99% eh, or more of the attacks that could happen. The only eh, small percentage left is eh, reliant on the user himself. So, for- And that's why a company needs to always provide training, needs to always provide local services, antiviruses and anti-spyware services. So, on my laptop itself, I have a smaller version of the antivirus, even though I am using a VPN. I need to have an antivirus on my laptop as a second layer of protection. So, if a hacker was able to hack the VPN connection, he cannot access my laptop.

X: What would be the difference of the antivirus on your laptop and the antivirus in the VPN?

Y: Eh, it could be just a different version. So, the VPN could be using an antivirus of eh, a specific provider, for example [software provider], and I am using [software provider], so I am using a different provider and this could provide eh, just an additional, different list of, of eh, protection. This is similar to any other services in the world. So, when you are having service from two different providers, you are using different features, which provide a better experience.

X: And what would be an attacker's intention?

Y: So, the intention is either eh, let me try to remember, so either for fun, just people who would like to hack, because they want to get the eh, recognition that I was able to do so, or for money, they hack to sell the information or to ask for ransom. Eh, a third eh, party, would be hackers who would like to blackmail, eh, to do an espionage eh, for governmental reasons. For example, [the professional services firm] is doing eh, providing services for governmental organizations, eh, and, so, they are foreign countries could hack to gain those kind of information. Eh, there is eh, the corporate espionage, so eh, eh, competing company who would like to eh, get the information or change the information of competing company. And I believe the last one is just for sabotage. So, for people who would like to destroy eh, specific information.

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

Y: It depend on the type of attacker. So, an amateur who would like to prove himself, he is just using his common tools, free tools that are on the internet, but if we are talking about eh, a government who would like to, eh, for example eh, the example of the American election, where Russia hacked the voting machines or where they hacked the process of the election. So, they have eh, open capabilities. They can do anything that you can imagine. So, it depends on the type of the hacker, the purpose.

X: And what could be the impact of an attack?

Y: Again, it depends on-

X: For [the professional services firm].

Y: Yeah. It depends on the purpose of the attack, it could be just eh, losing eh, a client data. It could be disrupting the business, and it could reach to eh, complete eh, shake in the credibility of the company. So, if it is a small attack on one laptop eh, one part of the client data would be stolen or destroyed, if the eh, attack is on one of the services that [the professional services firm] provides, they can disrupt their work for a day, or a week, or a month, until they are able to resume the work. But if the attack was on one of the critical services, this can make [the professional services firm] lose their credibility against their clients, and their clients are not trusting them anymore. And therefore, the security, of the eh, digital security is one of the top eh, priorities for eh, corporations, including [the professional services firm].

X: Clear, thank you. And this was all about social, digital threats, can you also think of social threats you deal with on a normal day?

Y: Eh, yeah, of course, there is always a threat. The threat of the eh, physical device to be stolen in public transport in eh, my locked car, if someone broke the window, to steal from the house itself. So, there is always the, the eh, risk of eh, the information being physically stolen. There is eh, other risks that are related to the social interaction. And for this, there are always, there is always a training on how to eh, maintain, eh, the secure information for the company and the clients. You are not allowed to discuss eh, client information publicly, with relatives, or with friends eh, in public locations. So, there is always measures need to be applied to protect eh, your, your information.

X: Clear, thank you. That were my questions. Do you have anything about VPN that you think eh, was not spoken now?

Y: Eh, I am trying to think if there is any other threats. Again, at this time, the use of external storage is being limited at the moment. [start drawing 4\_18]. But there is always the threat of accessing the data from an external source. Eh, either by an external hard drive, eh, an external flash disk, a CD, eh, any type of external eh, device. This could be a threat to the application or the data itself. With the, eh, more and more use of smart devices, you are not able to always use the VPN connection through those devices. so, there is always other measures to provide a secure environment eh, as if it for example, an, an, the mobile connection, you need to install eh, a certain application. So, for example an authentication software, or an encryption software, where it provides an extra layer of protection.

X: Okay, and can you think of anything else about the VPN you want to discuss right now?

Y: No, not at the moment. No, I believe we have covered most of the important eh-

X: Okay, great.

Y: Aspects.

X: Do you have any questions for me at this point?

Y: No, not at the moment.

X: Okay, then so far the interview. I will stop the recording.