# Transcription expert 8

Duration: 38 minutes

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

Y: It is a virtual private network. Eh, it is basically eh, secure environment, where connection happens. Eh, you can protect your information, you can eh, bypass your region of your laptop of your IP address. It allows you to navigate protect in the eh, in the internet. And it is usually companies require you to use when you have, when you work outside their secure environment.

X: Okay. You said a secure environment, what do you mean with this?

Y: Eh, secure environment is an environment in which you can be I would say protected from external eyes. For instance, man-in-the-middle attacks or people that are eh, like seeing your information. Sorry, it is a bit difficult in English. Eh, people like seeking information or spying on the transfer of packets, where they are transferring from one terminal, one terminal to the others. Like for instance the [the professional services firm] intranet network, then you are supposed to turn on every time that you work at home.

X: Okay. And you say you can use it to protect your info, how can that be done?

Y: Sorry, what?

X: You said it, eh, it can be used to protect your info, how can that be done?

Y: Because eh, the VPN works, there is codes via tunneling, the process, so there is, it protects the information, the transmit of the package from your let's say, your starting point to the ending point. For instance, could be communication between servers or from a website it protects the or it confuse your region IP. For instance, I can visit a website now from The Netherlands, but with some VPN connection I can make eh, I can appear as for instance I am in Italy or eh, something. So, this is through the tunnel, the tunneling process.

X: What do you mean with tunneling?

Y: Eh, it’s like eh, the way how is the VPN, the way the VPN works, so, it’s like protected, like the package that you are sending from one terminal to another is protecting from eh, external attacks. Like they are- You don't have, you don’t see the information so, when packages travels towards the internet, you usually can see like IP or eh, some information. Eh, but if you are, if you are doing via VPN and you are external observer, you don’t see this kind of information passing through from one point to the other.

X: And how is it that you can see that?

Y: If I can see what? The-

X: The IP address or the location.

Y: With the VPN or without?

X: With the VPN.

Y: Eh, no, sorry, I- Can you reformulate it? Like-

X: Yes, we can come back to it later otherwise. You said you can bypass your regions IP address-

Y: Yeah.

X: How can this be done?

Y: Eh, via protocol, like, you have specific protocols eh, and that can hide the IP address. Now, I wouldn’t know specifically which one, but I know there are some VPN services that allows this.

X: Okay, thank you. And you said it helps you to connect from one terminal to another, what do you mean with that?

Y: That it is the way how they communicate. So, for instance from, it's like a private channel from one input to the other input when you transmit the information. It's creates this, this private eh, private tunneling that is invisible to other people. Like to other, for instance, an attacker is watching, it doesn’t see the information, can’t grasp the information in the middle.

X: And why do you use a VPN?

Y: To protect confidential information, for instance, yeah, when you work in a company and you need to communicate with outside or for instance, as now working, smart working from home, you need to have your secure environment when you deal with eh, confidential information. So, to protect.

X: How is it then protected?

Y: How is, sorry?

X: How is it then protected?

Y: Eh, because you have no, because you have just eh, a VPN, then it is protected.

X: Could you explain how it is protected?

Y: Eh, because you eh, eh, you protect your information by hiding the content to outside eyes.

X: Okay. And how are you hiding the content?

Y: Through the VPN system. Am I repeating myself, because the question are like the same or it is supposed to be like this?

X: Yes, a bit. But that is no problem. Eh, we can go on to the next questions. What actions do you- Or, are there any other purposes for which you use VPN?

Y: Eh, more, it is, it depends on what you need. If you mean like protect your information, that is basically the main purpose, or if you want to eh, yes, hide, like, navigate in, not incognito mode, like hiding eh, some kind of eh, of eh, information as we were mentioning before the IP address. Basically, I would say it is generally for protection and safety of what you are transmitting.

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

Y: Eh, set up server, asking somebody, I am sorry, I am not technical on that. Eh, but you have to, yeah, you have to require a service provider, you need eh, specific eh, I wouldn’t say app, but device or it could be like a website, when you have connection for instance, [0:09:22 till 0:09:30 has been omitted].

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

Y: Sorry, the voice skipped.

X: O, sorry. As a user, what actions do you take to create a VPN connection?

Y: Eh, as I user I need to start like username, password, eh, maybe also have a code for instance. Eh, there is like token that you need that change every single time that allow you more eh, protection in case your eh, like eh, double eh, multi-factor eh, multi-factor eh, authorization. And is eh, yeah, for instance, we have like the key or the token for [the professional services firm]. Eh, yeah, it serves, it is additional steps to protect eh, in case you have, you lost your laptop or they steal the token.

X: What kind of token do you use?

Y: I use, it's a small device with a self-generated number every single time. So, it is four or five eh, [0:10:54 till 0:11:00] is number, like random number plus a fixed password.

X: Okay. And do you know whether there are multiple tokens in [the professional services firm]?

Y: Eh, yeah, there is, I think there is also something combined with an app. Eh, but I am still not using that.

X: And on what devices do you use the VPN?

Y: Eh, device, it is [access token provider], I think token.

X: Yes, and on what devices do you use the VPN?

Y: On my laptop.

X: Do you use it on any other devices?

Y: Eh, no.

X: And you said it a bit already, but can you explain to me how a VPN works? You can, if you would like, use the whiteboard for this.

Y: Eh, can I draw also?

X: Yes, you can.

Y: [start drawing 8\_1].Okay. So, so, if this is my laptop and I need to transmit to server, and this is the connection is what I have. This is the package in here, this is the tunneling, they are protected from whoever is looking from the outside and this is like internet. Okay, not very- I hope it is clear.

X: Yes, it is clear. Could you explain to me what a server is?

Y: O, god. The server is terminal that sends out or in information once requested.

X: Okay. And in this drawing, how would it look like if you access an internal application?

Y: Sorry, if?

X: If you access an internal application.

Y: If I access- I am sorry, because the, the audio is not very clear. If I access internal application?

X: Yes. How would this look like in the drawing if you access an internal application?

Y: Okay. Eh, it will be inside from eh, inside the same, I would. No, it would be the same, because I need anyway to connect to a server to have that information that I need.

X: Clear, thank you. And in your drawing, you describe the internet as above the VPN, do you do that on purpose or what is the relationship between the internet and the VPN?

Y: [start drawing 8\_2]. It is like this. Internet, like it is- No, I just randomly am putting there, sorry. Internet is everywhere I would say, so, it is not the-

X: Okay, clear. Thank you. And you said the package are protected by the tunnel. How are the packages protected by the tunnel?

Y: Because of the eh, of the private channel. Like, when information transits inside the tunnel, they are private, so this is, they become invisible to people from the outside.

X: How do they become invisible?

Y: Because of the, they are eh, use eh, they are coded, I don't know if it is the right word in English, eh, they are, they have, for instance, when you have HTTPS, before a website, like on the eh, on the link, it is like eh, yeah, it is coded. Cypher, they use cyphers. I don't know if it is the correct way to express it.

X: Clear, thank you. And for your computer, does it matter on which physical location you are?

Y: For my laptop?

X: Yes. Would the drawing change if you go to a different location?

Y: Eh, no.

X: Okay. Eh, I am going to ask a question in a different direction. What is the influence of a VPN connection on your computer security?

Y: Well, technically it is supposed to make it better. Eh, because protecting information, you should also be able to recognize malicious threats eh, or at least protect or raise a flag. So, eh, I would say it would increase.

X: How would it recognize threats?

Y: Eh, hopefully having a very good eh, antivirus. No eh, like avoiding website that you don’t know, opening emails from people you don’t know or look suspicious, avoid the eh, phishing, phishing website, phishing emails, just trying to be careful. Don’t link, or like don’t click on whatever link people send to you even if you have VPN connection.

X: What is the role of the VPN connection in this?

Y: To add, I would say, add an extra layer of protection of any communication you can have with eh, like with eh, confidential information. For instance, if I think about communicating with my clients by sending an email to them without eh, being connected to either VPN [0:18:28 till 0:18:29 has been omitted] from the company, it increases the risk of someone being able to exploit the email or to see what there is actually written inside. Eh, instead adding the VPN, adds an extra step in hiding confidential information.

X: Okay, and how- You also said it can help you recognize a threat, how does that work?

Y: Sorry, I also have to recognize?

X: It helps you to recognize a threat-

Y: No, I was expressing wrong, sorry.

X: Okay, no problem. Was just trying to clarify that.

Y: Yeah.

X: Okay. And eh, what else eh, what are the other influences of a VPN connection on your computer security?

Y: What, I am very sorry, it is just the audio, what?

X: What are the other influences of a VPN connection on your computer security?

Y: Eh, I wouldn’t know. I would just stick with protection. Increased layer of protection.

X: You mentioned antivirus shortly as well. Does that have a role?

Y: Eh, no, I mentioned antivirus when you asked how you can recognize a threat.

X: Okay.

Y: That was not linked to the VPN.

X: Okay. Then that's clear as well now. Eh, then a broader question. What kind of digital threats do you deal with on a normal day?

Y: Eh, could be eh, most of all it is trying to eh, avoid people to eh, exploit your information. So, phishing emails eh, trying to make sure I am not, from my point of view, I am not texting confidential information in emails or sharing- Eh, I would say that from my position it would be more trying to not leave my eh, my laptop open or without a password or eh, yeah, I think generally in my small let’s say, I would say more attack from the outside as like people reading something they are not supposed to. Eh, so yeah, just phishing, I would say phishing.

X: Okay. And does the threat, or if you think about these threats, do they change because of the VPN connection?

Y: It is not that they change because of the VPN connection, because they can still attempt to do it. Like for instance the man in the middle attack, he might does not know that there is a VPN connection, so, usually they, how they operate is, let's, basically let's try to say in the middle of this transfer and let’s see what are we able to catch from that. Eh, they might after, I would say that in the initial stage, they don't change. Of course, if you realize that somebody has a VPN connection, and you want absolutely exploit that person or that company, you should maybe think about something also physical for instance, using something from social engineering. Being able to actually exploit, I don’t know, using the USB, so, not mere digitally.

X: Okay, and if you think about these non-digital threats, does the VPN connection have any influence on those?

Y: Eh, no. On non-digital threats, no. Because if I steal your laptop, and you have documents in their without no encryption whatsoever, doesn't, yeah, I don’t need the VPN connection for stealing that.

X: Clear. And eh, if we think about these threats, who or what could be an attacker behind those threats?

Y: Who is the VPN attacker?

X: Yeah, the VPN attacker or the one performing a social engineering attack.

Y: I would say it is somebody- Depends, people do it for various reasons. Usually it is for money, very few people do it for seeking truth or whatever. Eh, it is more for blackmail and exploit the victims for money.

X: Okay. And could you think of other motivations?

Y: Eh, no, because at the end it is all about money. Even if I steal money and power, you have confidential information about somebody that you could use at any time if you don’t do whatever they want. Eh, no, because most of the, also most of the attack are, very few are just to disrupt some environment or company. It is more because you want something in return.

X: Clear. And who would want something in return. Who would be the attacker?

Y: Depends. People activists, people that want money for their own costs, people that just, like, scriptkiddie that wants just more money at the end of the month. There could be lots of reasons. Depends also for the company, like who is the victim, usually if the victim is like a state or, a government body or agency, usually it is more to expose them. Eh, like you, maybe they are activists, they do it for having something in return, like for their costs to use the money. Could be to undermine someone else's government eh, if you are just somebody that wants to blackmail a random CEO, you'd do it for money. Yeah, depends, depends on what you are looking for and what your end goal is.

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

Y: Capability?

X: Yeah. So, what would they need to be able to do to successfully perform an attack?

Y: With a VPN you mean?

X: Yes.

Y: Depends on how good you know your target. And how much resources you have, how much good you are and if you have, sometimes it helps to have someone from the insight. Eh, definitely it is not something you do from one day to the other. You need a bit planning about that. But I wouldn’t say it is not impossible. Because if you think recent privacy scandals about stolen data and confidential information, I probably would say also those companies had VPN and that didn't help much.

X: Would there be some kind of basis background you'd need as an attacker?

Y: Eh, background in, well, if you ask any hacker, if they have like background as a study or something, they will tell you no. They just start to hack, learn on the ground. Are you meaning background of the attacker personal or background on the victim of the attacker?

X: The background of the attacker.

Y: Okay. Eh, well, not they, depends, it is not that everybody eh, sometimes the attacker are like really kids that spend their, their years in front of a computer learning, watching videos. They don’t have degree that match eh, hacking. For instance, it is not that every of them has a degree in computer science or something. So, no, you just have to have practical knowledge of the, of how a computer work, how a system work, of VPN. But it is not eh, something that you need to deeply study, I would say.

X: Okay, thank you. How does the kind of attacker change because of the VPN connection?

Y: How does, sorry?

X: How does the kind of attacker change because of the VPN connection?

Y: The attacker or the attack?

X: Both.

Y: Eh, well, the attack change, because, yeah, if you can't eh, take eh, the information while looking from the outside, you need to think differently eh, because it could be something that you didn't, you didn't eh, foresee at the beginning of your attack. So, as I said before, maybe you should consider to enter or to take, like, to steal the information of the company in other way. Eh, for what concern the attacker, I don’t think the attacker profile change if there is no VPN.

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

Y: The, sorry?

X: What could be the impact of an attack?

Y: Well, the impact of an attack could be eh, disruptive, could be stealing, could affect physically eh, laptop, like laptop servers, virtual environment, for instance you could strike it down, turn it off eh, block it, like you don’t have access anymore. Or it could not, you could also not even realize, and it could just be spying on your information, on what you're doing with your laptop or stealing everything, and you didn’t even realize they were in. Eh, modifying information inside your eh, your servers, your eh, yeah, your laptop. It could be a lot of different attacks that you could do. And lot of different outcomes.

X: Okay and eh, if we think about the VPN connection in itself, how secure is a VPN connection?

Y: In, sorry?

X: If we think about the VPN in itself-

Y: Hmhm.

X: How secure is a VPN connection?

Y: Eh, technically a lot. Because this is how, this is what the scope it is supposed to work. This the why has been created a VPN connection and the why you install it is to protect, but also, the strongest for instance, the strongest type of encryption could be exploited at some point with effort and patience. So, there is always a possibility, a small chance that something might not work. Nothing is secure at 100%, especially in cyber.

X: You mention encryption, what is the relationship between encryption and the VPN?

Y: The information transfer are encrypted.

X: Okay.

Y: You use encryption.

X: How does that help you?

Y: It helps, because if you don’t have, if you send from one point to another, information encrypt need to have like the key to actually read the encryption, if you don't, if you see from here, you just see a lot of symbol, let's say inside. So, if you don’t have the key to decrypt them, they have no sense for you. Have no meanings.

X: And if you think about the vulnerabilities you possibly mentioned of the VPN connection. Do your actions change because of those vulnerabilities?

Y: If change, sorry, if change?

X: Do your actions change because of these vulnerabilities?

Y: Eh, not really, because there are some vulnerabilities that I might not be able to control, for instance where the VPN server is based, who is stealing with, like who is the service providers, there are some things, usually it is a third party. So, I don’t have control over that. Eh, and it could not, could be something for instance eh, also where the server is located. If it just a country where protection is not really eh, in place, also, like, from the point of view of eh, confidential information. Eh, I don’t know how much eh, powerful, powerful or how much big the servers are. So, there might be eh, if the powers goes off. There are a lot of things that can happen that are outside the control of actually the user of the VPN.

X: Yes. And you say it matters who the VPN supplier is, why does that matter?

Y: Why does it?

X: Why does it matter who the VPN supplier is?

Y: Because the, not everybody as we know has eh, the same level of security, or have to respect by states or by law the same level of protection. So, for instance I expect that in, usually in Europe or in the US, there might be a big, like, higher level of requirements a company can ask when provide this kind of services. For instance, in other eh, in other it might be eh, more- If I have to choose between set a VPN service in [country] or in [country], I would probably wouldn’t go for [country], because I know that they are, there might be more implication politically. And if something happened, it might be more, it might be harder for me, from being based in Europe, to actually understand what happened eh, and where my, my information went. So, yeah, this is why it matters.

X: And can you think of any other yeah, risks or threats with VPN?

Y: Eh, they can trust some VPN that for instance eh, I know they do it anonymously, but they still collect information from eh, they use for statistic and everything, but we, yeah, I think everybody knows that is not a good eh, a good thing in any case to have information, even if randomly and anonymously. Because you also don’t know if what, actually the law on their side, for instance because of the location, you don’t know how much eh, anonymized the information are, to which extent they can actually collect this kind of information coming from you. I would say that all the risk could be related to privacy and eh, yeah, privacy and confidentiality.

X: Are there any other risks?

Y: Risk could be that someone breaks in in the server, like physically. Could be someone breaks in where the servers are and, I don’t know, like switch cables, but I think that would be too much eh, eh, movie, I would say. Because you are, you are supposed to have like secure physical environment when you keep this kind of eh, of server. It can happen, but also, statistically, it is less possible then a digital attack in this case.

X: Okay. Thank you. Those were actually my questions so far. Is there anything you want to say about VPN that did not, that was not spoken about now?

Y: Eh, no.

X: Okay.

Y: Everything.

X: Okay. In that case eh, I would like to thank you a lot for your participation, this helps me a lot.

Y: Okay, I hope so.

X: And do you have any questions for me?

Y: Eh, no. No.

X: Okay.