Ask Charly Leetham
Relax, You're In Good Hands

VPNS 101 with Charly Leetham

Transcript for Episode 1: What Do VPN's Do & Why Your Business Needs One

Welcome to episode one of VPNs 101 by me, Charly Leetham. In this episode, we are going to be looking at what VPNs do and why you need one. In fact, I'm going to swap that around: why you need a VPN and what they do. I like to give context before I give too much information. So this is a short episode. I try to keep all my episodes short so that you can get bite-sized amounts of information to digest without having to take it all in and forgetting bits and pieces of it.

Why You Need a VPN: Real World Examples

As with all things, I like to give real world examples of why we want to do something. I am sure you've all heard the stories of people who have sat in cafes, in airport lounges, connected to the public Wi-Fi, and had information stolen from them. It might not be that they've lost their credit card numbers, it might not be that they've had passwords stolen, but they have had emails intercepted. They've had data intercepted or had information taken from them and used maliciously, or modified as it's in transit.

Now that happens because on a public network you can have bad actors sitting there and just looking at the data streams. And when I say looking at the data streams, I mean digitally looking at the data streams and seeing what's out there that they can use.

Another real world example I can give is geo-locking. Hands up if you have gone to YouTube or you've gone to one of the streaming services and said, "I want to watch this thing," and they've said, "No, sorry, that's not available in your country." Or you've gone to a service to go and buy something and they said, "No, I'm sorry, we can't sell that to you in that country." And you really want to be able to get that information. You can use a VPN to help you get over the geo-locking situation.

Now, whether you should be doing it in those situations that I just gave you, I don't know. I can't tell you whether you should or shouldn't be doing it. I'm not going to provide any information around that.

I can give you a practical example where I was traveling overseas and trying to support a client here in Australia. I went to log in to the service here in Australia from an overseas IP address, and the system came back and said, "No, can't log you in from that IP address. We don't allow logins from that IP address." So I put in a support ticket and they said, "No, that's part of our support process. To be able to ensure that bad actors don't get into our system, we have locked down logins to only IP addresses within the country."

Whether that's a good thing or a bad thing, it's a thing. And what I ended up doing was running up my VPN, connecting to a server in Australia, getting an Australian IP address, and then logging into the system that way. Whether that is really secure or not, it certainly made me jump through hoops to do it.

So there's two real world examples of how you can use VPNs and why you might want to use a VPN.

How Do VPNs Work?

Hopefully this diagram actually lands for you guys. I always struggle a little trying to get the concepts across because I think a little differently to people. When I look at this stuff, I go, "Oh yeah, that makes sense."

Let's take the VPN server here in the middle out just for a moment. Just pretend it's not there. And what you end up with is your device connecting straight into the internet, and your data will go from your device straight into the internet and from the internet straight into your device.

Now, when I'm talking about your device, if you can imagine this little U-shape here or arch, this is your router. It's still going through your router, so we've got a little bit of protection on your router, but not a lot. You're still connecting straight into the internet and straight back. The IP address of your router is exposed to the internet. If someone wants to follow your traffic back, they will follow it right the way back to the router. If they want to get into your device or try to find your information, they can try and hack your router to get through to your device. So you've only got one layer of protection, really. Maybe it's a little bit more depending on who your ISP is, but you've got limited layers of protection between your device and the internet.

It's also exposing your IP address to the internet. IP address—for those of you that are saying, "Charly, you're using jargon" (I do have podcast episodes on this that explain it a little bit more)—but your IP address is basically the numerical identifier for your device to the internet. It's like giving your street address out to people. It's like saying to people, "I live at this address here." That's the closest analogy I can give you.

What a VPN server does is it blocks itself, or you plonk it in between your communication stream and the internet. Your device and all the data from your device ends up connecting to the VPN server. The VPN server will terminate your communications at its edge and send any information back to you. And then after it's terminated, it creates a new data stream out to the internet and back.

If you send data in here, you send the data in, it stops it here, it transfers it through all of its little logic gates and whatever, and then when it communicates back, it goes, "Oh yes, that's with this data stream," and through all its logic gates and such in the server, sends it back to you.

It is creating essentially a digital air gap between your device and the internet.

You will notice that I also have green and red data streams here: encrypted and unencrypted. For the purists that are going to start screaming saying it's not really encrypted data here—correct, it is not encrypted data in that every byte or bit that goes out is encrypted or has a cipher applied to it. What it is, is that each unique transmission of data has a lock on either end of it, has a cipher on either end of it. For the data to be able to be used, the end device, the device that it's going to, has to be able to unlock that cipher to read the data.

So the data—we call it a tunnel. You ever hear someone talking about a tunnel? That's what we're talking about. The tunnel itself has got locks on it so that to be able to put data into it and to be able to take data out of it, you've got to know what the code is to be able to do that.

So the data between your device and the VPN server is encrypted at the communication layer, at the transport layer. We say that it's unencrypted out into the internet in that it can go out. And I'm trying to be a little less specific here, and it's not going to land as well, I think we'll see where this goes.

It's not unencrypted in that it's all out there in the open and everything is readable, because some of the devices on the internet, some of the hosts, some of the services—a lot of the services now that you connect to on the internet—use SSL. I'm sure you've heard that term: Secure Socket Layer. And that provides a level of encryption for the transport as well. So it's not totally unencrypted when it gets out here. And I really want to make sure that that lands with you—know it's not all unencrypted, but it is far less secure than this tunnel here.

So the idea of the VPN server is that it sits between you and the internet, and it will take your data stream, it will stop your data stream and start a new one and connect it up using logic so that there is no direct correlation between your device and the traffic stream that is out here in the internet.

What VPNs Do

Let me move on to the next slide because that gives me the next set of talking points here. So what putting that service, that server (we call it a server, it's actually more of a service which has a number of servers) does is:

- **Helps you secure your public Wi-Fi** because you get that encrypted tunnel from your device out into the internet. It makes it much harder for someone to break into your data stream and find any information in it.
- **Hides your IP address from the internet.** It will hide your device—not necessarily your device's IP address because that's already hidden behind your router—but it will hide your router's IP address from the internet.
- **Allows another level of obfuscation.** So it will obscure where that data stream is coming from.
- **Encrypts the data stream** as I said with securing your public Wi-Fi. It makes sure you've got a level of protection.

The thing that I really want to point out here and hope it lands with you, I hope it really makes sense to you, is: **it makes things more secure. It doesn't make things 100% secure**.

It is incredibly rare you will have me say, "This is unhackable. This is just totally secure. No one will be able to get in," for a couple of reasons. One is, basically nothing is ever 100% secure. Secondly, even if it was 100% secure, it will probably only be that for a matter of seconds.

I always use the term: if you build a better mousetrap, you end up getting smarter mice, because they will find ways around it. If someone wants to get into something, if someone wants access to something that badly, they will find a way of doing it.

The whole thing with IT security and security in general—think about your physical security as well, and by physical security I mean the locks on your doors and your alarm systems and such—the whole idea with security is that you make it hard to get in. You make it take a lot of effort to get in. Someone has to put in a whole heap of effort, and hopefully they go, "You know what? This is too hard," and they go elsewhere. Or it's so hard you delay them long enough that you can actually deploy anti-intrusion measures to kick them out and stop them getting in.

So when I talk about security and saying things that are secure, what I mean is that it's much, much harder to get access to information and to do things. Not that you're not ever going to get hacked because of this. But that's what a VPN does. It adds that extra level of security. It adds that extra level of digital air gap between your computers, your devices, and the internet.

What VPNs Don't Do

These are things that VPNs don't do, and we need to touch on the things that they don't do so that there is no confusion.

A VPN only ever looks at the transport layer, the data layers. It doesn't look at the application layers.

When we talk about applications, we mean things like your email: Outlook or Gmail or Zoho Mail or whatever you're using. Word documents, Excel spreadsheets, Google Docs, Zoho WorkDrive, anything that runs as an application. VPNs typically don't look at those, so:

- **They can't help you with phishing emails.** They can't help you detect phishing emails. They won't stop a phishing email getting in. They won't highlight that this is a phishing email. It really doesn't care. It's just looking at ones and zeros. It's just going to send that through to you.
- **It won't help you with viruses and malware.**
- **It won't help you if a hacker already has access to your computer.** If they've got access to your computer, they're going to be able to get access again.

So that's what a VPN doesn't do. What it does do really well is help you protect that data before any of this happens.

Summary

So in summary, what we've spoken about today is what is a VPN and why you want to use a VPN. You want to use it to increase your security, increase your anonymity as well, and give you a level of obscurity between who your device is, where your devices are, who you are on the internet. So if someone wants to follow that data stream back to you, it's really hard because they get to the VPN server and go, "What? Where does it go from here?"

We've spoken about how that works, and we've also spoken about what a VPN doesn't do.

Connect With Me

If you guys want to know a little bit more about me, if you want to get in touch with me, if you've got questions that you want to ask, you can connect with me in any of these locations. You can follow me there. I would really appreciate the likes and follows - it really does help.

You can also join my community at AskCharlyLeetham.locals.com and have conversations there. If you scan that QR code, it will take you to a page on my website which has all of this information that you can just click on.

https://askcharlyleetham.com/connect-with-me

Next Episode

In our next episode, we're going to be talking about the shady sides of VPNs, the things that you need to consider, the things that you need to look for and avoid when you're buying a VPN.

I will see you all in the next episode!