At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one online risk of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What parents need to know about VPNs

Although a great privacy tool in the right hands, VPNs can be dangerous for children and let them bypass restrictions you have on web browsing.

What is a VPN?

A Virtual Private Network (VPN) is a privacy tool used to hide internet activity from prying eyes. Without a VPN, internet traffic is sent directly from your computer or smartphone, letting anyone in-between you and a website or service that you're accessing (such as a wireless hotspot owner or your ISP) see what you're doing. With a VPN, a secure tunnel is created between your computer or phone and what's known as the endpoint. The endpoint is merely the part of the internet where your connection comes out and can be in the same country as you or located anywhere else in the world.

Using a VPN has two main effects. First, as the tunnel is fully encrypted, nobody between you and the final endpoint can see what you're up to. Secondly, as all of your traffic looks as though it's coming from the endpoint, you can further avoid being tracked and monitored, hiding your real location from everyone.

VPNs have many legitimate uses. For example, running a VPN when on a wireless hotspot or hotel network that you don't trust, gives you additional security. There's also improved privacy by using a VPN, preventing ad networks and the like from tracking you and working out where you live. VPNs are also often used to bypass protections, say watching UK streaming TV when abroad by pretending that you're still in the UK.The way a VPN works means that children can also use VPNs to hide what they're doing and get around any restrictions that you might have in place.

National Online Safety®

Publish date: 20/03/19

MEET OUR EXPERT

This guide has been written by David Ludlow. David has been a technology journalist for more than 20 years, covering everything from internet security to the latest computing trends and the smart home. A father of two (a nine-year-old and a six-year-old), he's had to control and manage how his children access online services and use apps.

What are the risks?

There are three main issues with VPN usage by children, potentially affecting their privacy (and yours), and opening them up to seeing inappropriate content.

1) Viewing age-inappropriate content

Parental control tools work by looking at the sites that a child is trying to visit, and then blocking according to a list of what's not allowed. With a VPN, the secure tunnel that's created means that web traffic can't be viewed, so parental controls stop working. Once on the open internet, a child using a VPN can look at anything they like unrestricted. This isn't just at home. Children that are allowed to take devices into school for work purposes can also use VPNs to bypass any filters that have been set up on the school network, too. VPNs can both be in software and via what's known as a proxy website. With a proxy website, a child visits this, then enters in a blocked website address that they want to view. the blocked website is then downloaded and viewed through the proxy, sidestepping any parental protection.

2) Malware infections

Installing any unknown application is fraught with danger, and the same applies to many free VPN applications. In an investigation, it was found that 38% of free Android VPNs contained malware, with 75% also designed to track activity. By installing suspect software, a child may be opening themselves up to being spied on and their private details being stolen. If you use a shared device with a child, an infection can also affect you. Malware can spread, and there's then a higher risk to other devices on your network. There's a chance that a dodgy VPN will use your computer and internet bandwidth, too. Back in 2015, the free Hola VPN extension was found to be secretly selling its users' bandwidth via another service and, in some cases, users' internet connections were being used for illegal activity.

3) Free VPNs can spy on people

The best commercial VPNs are built around privacy and have strict rules about hiding activity, not spying on users and not logging data. These tools are built for adults who wish to protect their anonymity. Children often go for free VPNs and proxy websites, which have a less strict code of ethics. Many free VPNs have been found to spy on activity, store private information and even sell this data on. When using a VPN like this, dodgy adverts and pop-ups can be inserted into web traffic, beyond the harmful things that your child may already be viewing.

What parents can do

Although the risks might seem entirely different, the protection from VPNs is the same for all of the threats.

OFF

ON

Filter VPN sites

Check the parental controls software that you're using to see if there's a filter to block VPN/Proxy traffic. If this is selected, it will prevent most known VPNs from working, along with proxy websites.

Block VPN applications

Stopping and removing any VPN applications running on a child's device is a must. If you have parental control software that can restrict application use, make sure that you investigate any application that your child wants to install and block all VPNs. If you've recently enabled any applications, go back and check what they're used for and remove any VPNs that you find. If you don't have software to check what's running on a child's devices, then you should manually check. Searching for an application with VPN in the name is a good idea. Look out for tell-tale signs, too: computers and phones will usually display a different connection symbol when a VPN is connected. You can also use a child's computer to try and view a restricted website to ensure that filtering is still in place.

Monitor your child's online activity

In order to prevent your children from falling prey to inappropriate content, it's important to monitor your child's internet usage and have open and honest discussions with them about their online activities.

Sources:
www.safervpn.com/blog/use-free-vpn-hola-risks-cybercrime/
https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf
www.pcworld.com/article/2928340/ultra-popular-hola-vpn-extension-sold-your-bandwidth-for-use-in-a-botnet-attack.html

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 20.03.19