LINEWIZE
by family zone

DIGITAL TECHNOLOGY OVERVIEW

Student Use Of VPN Agents to Bypass Internet Filtering

An introduction to the challenges faced by schools in ensuring appropriate internet use in BYOD environments where student devices can make use of VPN software.

Introduction to VPN-based Filter Avoidance

The rapid adoption of digital technologies in education introduces new challenges for schools looking to provide a safe online environment.

As schools adopt BYOD (Bring Your Own Device) programmes and invite student devices onto their networks, a number of new threats emerge that many schools are unprepared for.

Student devices differ in that schools have no control or visibility over what software might be installed on them. One type of software application that has particularly concerning implications for schools are VPN (Virtual Private Network) clients.

Traditional use of VPN software is popular for many constructive purposes including:

- Remotely accessing files on a private network
- Protecting online privacy when using public WiFi networks
- Gaining unrestricted internet access in countries that restrict use

Unfortunately the ability of VPNs to allow access to any online content is particularly attractive to many students wanting to bypass existing school internet filters.

Over the past two years, Linewize has measured a marked increase in the adoption of students using VPNs to bypass traditional school firewall internet filtering.

Analysis of student VPN use across 260 New Zealand schools has shown that up to one third of secondary school students have used VPN software in an attempt to bypass their school internet filtering system. This has now reached almost epidemic levels, with such behaviour becoming normalised across the student population.

Traditional firewalls such as the free default filtering provided to New Zealand schools fail to provide an effective VPN blocking solution. Schools looking to uphold their duty of care must ensure that students are not able to use filtering avoidance technology to bypass their internet safety policies.

The National Administration Guidelines (NAG's 5) state that schools are required to provide a safe physical and emotional environment for their students. Schools have the responsibility and the power to act when any such content could reasonably be expected to impact negatively on the school learning environment.

The Extent of School Responsibility

The recent Digital Technologies in Schools Report shows that of the 464 schools surveyed across New Zealand, only one quarter of school principals had full awareness of their responsibilities under the Harmful Digital Communications Act.

This legislation was designed to crack down on cyber-bullying, enabling civil and criminal action to be taken against harmful online behaviour. Around 100 prosecutions have been made so far, with serious offences attracting up to two years in jail or fines of up to $50,000.

One in five principals reported that ALL students in their school have access to a personal digital device, suggesting a more proactive approach to personal digital device management is required. While three-quarters of New Zealand schools have an ICT Strategic Plan for the deployment and use of digital technologies for learning, including policies for safe digital learning environments, only half of these schools actually have specific policies in place regarding the use of personal digital devices for learning.

It is clear that principals need to consider the legal implications of student VPN use to gain unfettered internet access to misuse the school network for harmful and anonymous online activities such as online bullying.

VPN Use and Digital Distraction

Our analysis suggests that the majority of student VPN use is driven by the desire to access social media, games and other media that the school has deemed unrelated to learning activities.

Schools are increasingly finding that this kind of digital distraction can be a major issue in class. In a recent publication titled ‘The relative potency of classroom distracters on student concentration: We have met the enemy and he is us.’ the authors rate self-produced distractions, such as playing games, checking emails and surfing the net, as the most common classroom distractions, with more than a third of students admitting to ‘multitasking’ in class time.

Alongside this, academic evidence is pointing to the detrimental effects of distraction. Research is demonstrating that multitasking is not an effective way to learn and will ultimately affect achievement. Leading expert Dr Larry Rosen, a psychology professor at California State University, refers to it as ‘Continual Partial Attention’. He strongly advocates that if we want students to learn and perform at their best, smartphones and other online distractions must be managed.

Research into the attitudes of teachers around the globe shows that the education profession agrees. Last year, an international survey of more than 2,000 teachers reported that 62 per cent were most concerned about distraction in class, more so than privacy and security. Yet 74 per cent of these still believed in the potential future benefits of these devices.

To address classroom digital distraction concerns it is imperative that student VPN use is blocked to keep student attention on-task and lesson focussed.

A New Paradigm in VPN Blocking

Traditional filtering solution take a reactive approach to identifying VPN traffic on a network. Incumbent network equipment vendors spend time reverse-engineering VPN technologies in order to create detection signatures that are then pushed out as filtering updates with the intent to curtail VPN activity. This manual approach is inherently time consuming and makes it impossible to keep up with every changing VPN traffic.

Schools need to keep up-to-date with the latest filtering avoidance practices, block VPN use, and support a safe learning environment for all devices, student or school-owned.

Conclusion

Schools are facing increasing challenges to fulfil their duty of care to provide a safe online environment for students and staff. Without adopting an effective solution to block VPN use it is impossible to ensure student internet use is safe and education-focussed in a BYOD environment.