BIZCOMMUNITY

What are the cyber risks of online schooling?

By Doros Hadjizenonos

4 May 2020

With lockdown forcing schools and tertiary institutions to take learning online, a plethora of new risks are facing children, families and learning institutions.

It's now estimated that 70% of students worldwide are currently doing some form of online education, and South African learning may see some – or all – lessons taking place online for the foreseeable future.

For many institutions, the switch to remote learning was unexpected, leaving little time for them to mitigate against new cyber risk before their students went into the virtual environment. But as online learning becomes a new normal, there are certain risks to be aware of:

- **Cyber bullying:** younger children who may not have had access to online social platforms are now entering online class chats and study groups. Teachers should moderate these carefully, and parents should monitor what is being said in these forums, and who has access to them.
- **Phishing:** learners with un-monitored access to online gaming, email and social media can easily be tricked into clicking on unsafe links or sharing personal information. Parents and teachers need to educate young learners on phishing risks and the importance of keeping personal information private.
- **Hacking the home:** children falling prey to cyber criminals can give hackers access to the family network, which is shared by parents working from home. In this way, attackers could potentially also access parent's corporate data and networks.
- **Hacking learning institution networks:** unsecured school networks present the risk of hackers accessing students' personal data and results, as well as the financial systems of the institution.

To mitigate these risks:

- Education and awareness is key. Learning institutions should host information sessions for both parents and learners

about cyber risk and how to guard against it.

- Institutions should provide strong authentication policies, and even multi-factor authentication where possible to prevent the misuse of stolen passwords.
- Protect web applications: Next to stealing credentials, exploiting vulnerabilities in applications is the easiest way for an attacker to breach the network. Institutions should have a web application firewall (WAF) in place and need to scan external sites for security flaws such as cross-site scripting errors and SQL injections. They should also encrypt and monitor the traffic between learning systems and users.
- Use network segmentation: By segmenting internet-facing teaching applications from other internal applications, such as the HR system, the scope of impact will be limited should a breach occur.
- Manage third party risk: The third-party technologies that you use in your online learning environments can pose additional vulnerabilities and risk to your enterprise network. Learning institutions should raise user awareness of the risk of spoofed sites and applications, and share access with authorised and secure tools.

While large institutions such as universities likely have IT security capabilities, many schools and parents are now navigating the cyber risk environment for the first time. Education and awareness are crucial for their online security – they need to practice basic security principles and at the very least they should ensure that learning devices and applications are updated with patches, and that any antivirus/malware software is current and operational. It is also essential that any distance learning tools – both the front end used by students and the back end used by teachers – support SSL VPN and strong authentication.

ABOUT THE AUTHOR

Doros Hadjizenonos is the regional sales director at Fortinet.