Barracuda

PARTNER LOGO

Defending Remote Learners from Web-based Attacks

In today's online education environment, you can never tell the number of websites users visit every day, and how many students, teachers, and academic staff are engaged with social media every moment. But are they 100% secured? Protecting remote learners and staff is critical when e-learning becomes the new normal during the pandemic.

Microsoft Security Intelligence has discovered that most computing devices in the education sector become infected with malicious adware, which not only overrun the devices with unwanted advertisements, but also drop trojans in the machines to open a back door for future cyberattacks. There are also cases where user devices have been invaded by ransomware or other malware through social media or compromised websites unconsciously facilitated more tremendous attacks on the school network, resulting in disastrous consequences.

Maintaining a secure computing environment for school users on and off campus is an urgent matter that admits of no delay. Let's welcome our FBI!

1. **Filter** harmful URLs, web content and traffic, and online activities
2. **Block** malicious content and applications which carry web-borne threats
3. **Identify** inappropriate user behavior, dangerous network activities, and content policy violations

You need the FBI in the cyberspace to protect your business. Barracuda gives you a content shield to prevent users from accessing harmful websites, and a web security gateway to stop web-based attacks. Take action today!

- **Get a free trial of the Barracuda Web Security Gateway**
- **Get a free trial of the Barracuda Content Shield**

Free Consultation

Forward this to a colleague