Barracuda

PARTNER LOGO

What is The Bitterest Lesson to Learn at School? Hackers will Let You Know!

Nowadays, with ransomware attacks escalating at an alarming rate, many people still believe that only businesses are being attacked. But the reality is, recent years have seen a sharp rise in attacks at schools, colleges, and universities. Don't think that attackers will spare education – it's a rich target as education institutions ramp up online learning. The collaborative data stored in commonly used cloud environments, such as Microsoft Office 365 is a rich target for attackers that want their victims to pay ransoms quickly.

"Don't worry, our data is protected."
Are you sure? Don't believe these misconceptions.

Misconception 1: Microsoft is responsible for backing up Office 365.

Reality: Microsoft is responsibility for service availability, not data backup and recovery – and says so in the services agreement.

Misconception 2: We can simply back up Office 365 data into the school's on-premises environment.

Reality: What if your on-premises infrastructure is taken over by ransomware or damaged in a disaster? Best practice is to have at least 3 copies of your data at all times.

One key point about any backup is that it needs to be "air gapped" so that if your school network is compromised the attackers cannot get from there to your backup environment and infect or disable it. Your backup is your last line of defense against ransomware.

Barracuda Cloud-to-Cloud Backup is the answer. Offered as software-as-a-service, it allows you to just log in, configure, and then back up data to the cloud easily – get started from signup to running your first backup in 5 minutes. You can restore the whole mailbox or individual emails, and SharePoint/OneDrive/Teams data and have total peace of mind against ransomware. Act now!

CONTACT US to find out more

FREE TRIAL

Forward this to a colleague

Privacy Policy I Unsubscribe