WHY IS THE EDUCATION SECTOR TARGETED BY CYBER CRIMINALS?

CYBERCRIME INDUSTRY SNAPSHOT

Education

CYBER READY

mailguard

The volume of **bring-your-own-devices**, **collaborative learning environments** and **open-access culture** make educational institutions a prime target for cybercriminals

From primary schools to universities, the education sector offers a goldmine of information that cyber thieves can exploit to commit fraud, steal identities and intellectual property or launch spear-phishing attacks.

Educational institutions have ubiquitous, mobile workforces and student populations. They tend to be heavy users of social, cloud-based apps, and open-source / commercial enterprise software. Large student and staff populations mean endless potential entry points for a cyber breach.

The volume of end-user vulnerabilities is growing, given the tendency towards bring-your-own-devices (BYOD). Millions of devices are brought inside school ecosystems each day, all connecting to public Wi-Fi networks. These users are transitory in nature, and might be accessing the network from anywhere in the world.

Millennials, forming a large majority of university undergraduate student populations, also use their own devices beyond the campus firewalls introducing new security concerns.

High-profile cybercrime incidents in the educational sector

paid by a college in Los Angelas

after hackers took control of Los Angeles Community College District campus' email and computer network.

in China infected by WannaCry

suffering serious breaches of research and personal data in 2017.

siphoned by spear phishing attack

MacEwan University Alberta, Canada: Staff transferred funds to cybercriminals in three separate instalments after being duped by an email impersonating a supplier.

lifted from a TAFE Queensland database

after their IT systems were infiltrated in 2015 by hackers, exposing numerous personal details.

Despite investing in antivirus solutions, the majority of universities say they are still affected by cybercrime, and suffer consequences with financial, business continuity, reputational, legal and regulatory compliance implications.

The cybersecurity landscape for education

Schools and universities are lucrative targets, rich with sensitive IP and personal data

Today, no industry is free from targeted cybercrime. The Education sector is a prime target due to the diverse range and quantity of valuable data, from coveted student records to classified research.

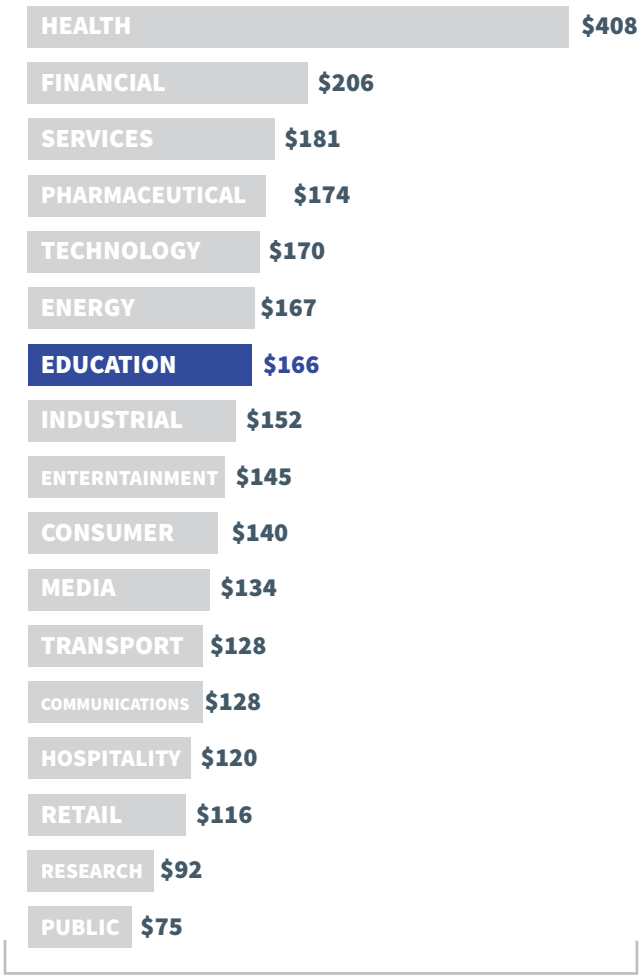
Protecting student populations from online predators is vital for productivity and security. Personally-identifiable information (PII) such as contact details, Tax File Numbers / Social Security Numbers, payment information, and academic records have high market value to cybercriminals.

High-profile university ransomware attacks

In 2018 the media reported a cyberbreach of Australian National University's IT systems. Infiltrated by China-based hackers, key national security and defence research projects were potentially compromised. The cyberintrusion involved the theft of data yet to be determined, as Australian Government cybersecurity officials continue to assess the scale of information theft, who is responsible for it, and when the attacks started to occur.

UK-based Bournemouth University, which features its own cybersecurity research centre, suffered 21 ransomware attacks over a 12-month period.

In 2016, The University of Calgary was hit by a massive malware attack, forcing the university to pay hackers a CAD $20,000 ransom equivalent to untraceable Bitcoins. The university are a regular target for hackers, receiving 10 phishing attacks a day on average.



COST OF A DATA BREACH BY INDUSTRY

Per capita cost by industry sectors
Measured in US$

Source: IBM Security / Ponemon Institute 2018 Cost of a Data Breach Study

MailGuard reporting on recent phishing scams

Cybercriminals impersonate brands that are household names and have large customer bases. The brand recognition, coupled with curiosity or fear, impel unwary recipients to click through to phishing sites, or inadvertently download executable malware. MailGuard has reported email scams purporting to be from government agencies (ATO, the High Court), popular online subscription or free services (Apple, Netflix, Dropbox, Office 365), delivery services (Australia Post, UPS, DHL) and telco / utilities (Telstra, Origin Energy).

Scams bank on human psychology to respond (e.g. tax evasion, traffic infringements, court order, unauthorised account login attempts, overdue bill), reinforced by sophisticated, well-crafted emails and phishing sites (often indiscernible from the mimicked sites). Unfortunately, these campaigns are effective, with 7.3% of targeted recipients successfully phished. The market value of PII on the dark web ranges from USD2,000 for a passport to USD1,065 for a medical record and up to USD400 for a diploma, so a successful phishing campaign can be a boon for cybercriminals.

Education sector testimonials

"Since implementing MailGuard back in 2005, we have seen an easy and trouble-free cloud email security solution we never need to worry about. It meets our needs in protecting TAFE students and staff from potential cybersecurity threats."

—Infrastructure Manager, Holmesglen TAFE

holmesglen

"Since making the transition to MailGuard from our previous provider there's been a massive improvement in our mail flow and quarantine management. Managing blacklist and whitelist policies have become simpler and much more flexible. I highly recommend MailGuard's email filtering solution to my peers."

—IT Manager, Rivermount Education

RIVERMOUNT

GET CYBERREADY WITH MAILGUARD

We identify and stop fast-breaking attacks in real-time, 2-48 hours ahead of the market

Contact your IT service provider now for an obligation-free, 14-day trial

PHONE 1300 30 44 30
EMAIL expert@mailguard.com.au
WEB mailguard.com.au

CYBER READY

mailguard