Back to school? Are you prepared to face the K-12 cybersecurity crisis?

Going back to school? There are a few questions you might want to know the answers to. What Anti-virus do you use? Is your device encrypted? How often do you back up your device? if you are thinking about what this has to do with school, think again. The K-12 cyber security crisis has been looming over the USA for a couple of years now, disrupting education and critical operations, exposing sensitive personally identifiable information of students, teachers, and staff, leading to high recovery costs and emotional pain.

Centre for Internet said incidents aimed at K-12 school systems could jump by 86% in the coming academic year. Microsoft Security Intelligence has said that K-12 cyber security attacks are higher than in any other industry. The number of attacks has been going up year over year and data about K-12 cyber security incidents are published on an enhanced interactive map. This map has been published by the K-12 Cybersecurity Resource Center and it paints a picture of the gravity of the situation.

Covid-19 and K-12 cyber security crisis

The COVID-19 pandemic brought new problems in the K-12 cyber security space., This can be seen in the frequency of cyberattacks, which followed the usual pattern until the second semester of 2020; after that, the pandemic hit, schools started opting for remote learning, and cyberattacks increased. This sudden increase in the number of cyber-attacks can be attributed to the shift to remote learning. Most of the devices used for online learning are personal devices. Without any kind of special security in place, they leave it vulnerable to hackers online. Hackers tend to look for weakly guarded systems and voila! school security systems answer their prayers.

According to CISA, 57% of ransomware incidents reported to the MS-ISAC in last August and September affected school districts. Numerous industry studies have shown growth in remote learning made school systems much more dependent on technology and greatly increased the number of vulnerable endpoints on their networks.

In the year 2020, K-12 Cyber Incident Map cataloged 408 publicly-disclosed school incidents, like student and staff data breaches, ransomware and other malware outbreaks, phishing attacks and other scams, denial-of-service attacks, and a wide variety of other incidents.

But why?

Due to the COVID scenario, schools had to increase their reliance on virtual learning and this leads to a lot of undesirable results such as –

- Deployment of thousands of devices to students and tutors, often under very tight deadlines.

- Altering teaching and learning techniques overnight without adequate training given to tutors and students.
- Users install random free apps without proper vetting, making devices vulnerable to cyberattacks.
- The IT department not being able to troubleshoot devices manually and being forced to deploy remote access tools online without proper security protocols.
- Devices were used on unprotected networks and home networks during remote learning. These devices are being re-introduced into the school grids without proper scanning for malware, making the school network vulnerable.

The impact

Data breaches have been the most prevalent sort of publicly-disclosed cyber event encountered by school districts since at least 2016, proving that they are a threat that must be addressed. Between 2016 and 2020, data breaches exposed the personal information of a large number of K-12 children. Grades, bullying reports, and Social Security numbers were among the data stolen, putting kids susceptible to emotional, physical, and financial harm.

The privacy of thousands of students, their families, professors, and staff were violated. They were vulnerable to internet abuse, fraud, and identity theft. With sensitive information being revealed online, college admissions and other sensitive processes, such as special education funding, were put in danger. Ultimately, data breaches harm the reputations of school districts and degrade community faith in the institutions.

Moreover, new forms of cyber events at school have emerged in the year 2020, such as 'Class invasion,' which is described as instances in which unauthorized persons disturb online courses, frequently with hate speech, startling pictures, sounds, and videos, and/or threats of violence. Another kind of attack is through 'Email invasion' which involves the compromise of a school district email system for the purpose of bulk sharing of disturbing images, videos, hate speech, and/or threats of violence or links to the members of the school/district community

Another possible threat is a denial-of-service attack, in which a server is purposefully overwhelmed with requests, causing the website to shut down. Hackers in this case target the school website or portals to render them useless.

Phishing assaults are one of the main reasons for many school security failures. An unsuspecting school district employee receives an email with a malware link in this hacking tactic. The user's device gets infected if he/she clicks on the link. This provides an opportunity for the hacker to break into the school district's network.

Phishing assaults are one of the main reasons for many school security failures. An unsuspecting school district employee receives an email with a malware link in this

hacking tactic. The user's device gets infected if he/she clicks on the link. This provides an opportunity for the hacker to break into the school district's network.
After breaking into the school's database, hackers use ransomware to encrypt the data and threaten to reveal private information unless the district pays the hacker's price.
Social Engineering is where the hacker impersonates a school employee or vendor to gain access to his login credentials.
All this happens because school districts have not prioritized stronger security and don't possess the liveware or resources to deal with such scenarios. However, cleaning up the losses after the breach is also financially taxing for the districts. In addition to this, the districts may also face state and federal penalties for failing to follow security precautions. So, the saying 'It's better to be safe than sorry' does make sense, doesn't it?

What can we do?

The same way as you eat right, exercise and maintain basic hygiene to stay healthy, there are ways you can drastically lower the chances of being a cyberattack victim by following a good cyber hygiene routine. Unfortunately, it is taken as seriously as taking a shower on a lazy Sunday, but this may change as cyber threats continue to evolve. In the meantime, establishing solid cyber hygiene practices should be as routine as brushing your teeth.

1. Install a trusted antivirus and malware software

Antivirus software is a program or umbrella of programs that scans and eradicates computer viruses and other malicious software or malware. It's a vital component of your overall cyber hygiene.
Specifically, antivirus software provides protection by performing key tasks like

- Automatic scheduling of scans, regularly scrutinizing and pinpointing the location of the malware and eradicating it
- It can scan either one particular file or your entire computer, or a flash drive, depending on your specific needs.
- It automatically detects and erases malicious codes and software.
- It gives you a detailed report about the 'Health' of the particular device that was scanned.

2. Use a firewall

Firewalls are a first line of defence in network security as it prevents unauthorized users from accessing your websites, mail servers, and other sources of information that can be accessed from the web.

3. Set strong passwords

A device needs to have a strong password, the password must be unique and must be a combination of text, numbers and symbols.

4. Update your device regularly

Update your apps, web browsers, and operating systems on a regular basis to guarantee you're using the most up-to-date software that's free of bugs. Setting this feature to update automatically will ensure that you have the latest security

5. Use multi-factor authentication

Multi-factor authentication helps secure the school portals by requiring users to go through at least two authentication methods before eventually logging on. This generally requires a user to authenticate using a second authentication method besides typing in the password, thereby providing a second layer of security. This is achieved usually with the use of biometrics, including facial or fingerprint recognition, to make it harder for hackers to gain access to your device and personal information.

6. Back up regularly

While having good cyber hygiene can be helpful, it doesn't guarantee the complete safety of your device, so it is better to back up regularly to avoid an unlikely situation where you lose all your important data.

7. Keep your hard drive clean

If you are going to dismantle, throw away or sell your old devices, always make sure you are reformatting and then wiping your hard drive clean. If there are a bulk of devices that needs to be wiped, UEM solutions like Hexnode can help you fast-track the process and format the devices in bulk. This ensures that none of your personal data is passed along or accessed by anyone picking the hard drive later.

8. Secure your Wi-Fi router

Always make sure you password protect the Wi-Fi router you connect to., This includes turning off and updating the default name and password the router came with from the manufacturer, turning off remote management, and logging out as the administrator

once it's set up. Also, make sure your router offers WPA2 or WPA3 encryption to maintain the highest level of privacy of information sent via your network.

9. Use a trusted UEM

Using a trusted UEM can go a long way in easing up all the above-mentioned tasks. As an IT admin, it can be a daunting task managing all the users and devices in your organization. However, an endpoint management solution like Hexnode can make it a breeze. Hexnode provides unified management of endpoint security, app and content management, remote troubleshooting, and more. IT admins can assign the devices to faculty or students by enabling grouping by class, usage, or state of the devices with custom tags, and deploy devices via Zero-Touch enrollment.
Various policies can be assigned to have complete control over what a user can do, like putting in place password policies, auto-updating the OS, blocking unknown apps and websites, among various other features which can help you completely secure the device. In terms of reactive security, Hexnode lets administrators know when devices move out of bounds from the assigned geolocation through geofencing.

Takeaway

It's established how important K-12 cyber security is and it is paramount that we maintain good cyber hygiene. With cyber threats rampant and on the rise, a security solution has become the need of the hour. Hexnode UEM is a handy tool IT admins can use to secure all their endpoints, always remember 'a stitch in time saves nine'.