The Five Scariest Threats to Your District's Network Security

More is riding on your school district's' network security than ever before: financial stability, community data, and even your students' future creditworthiness. Unfortunately, not all districts are equipped with the personnel and safeguards to protect their networks, so are exposing their communities to serious harm. Are you prepared to protect your district against these five common threats?

1 Cryptomining

This danger could be going on right under your nose—it's already secretly taking a toll on many education communities nationwide. Simply put, cryptomining is the process by which cryptocurrency miners hijack computers on your network—via a simple JavaScript, say, in your browser—to enlist them in currency mining efforts. This invasion costs your district money and jeopardizes your security.

In addition to promoting best practices among your users, traditional malware defense systems may help prevent cryptomining—but not all systems are up to snuff or do more than treat the symptoms. It is imperative, then, to make sure your network deploys a defense system that specifically targets cryptomining attacks. Especially effective are Domain Name Service-based protections.

2 Wiper Ransomware

Ransomware attacks, incidents of which have more than doubled over the past year, are bringing organizations of all kinds—educational, governmental, corporate—to their knees. In a typical attack, malware captures an organization's data and hides it behind an encryption key to extort millions to recover the lost information. Worse, in the increasingly common "wiper" ransomware attacks, the infecting malware wipes your back-up system clean before holding your data hostage.

3 Student Data Loss

Best use practices help mitigate the risk of ransomware attacks, but such practices are not in themselves sufficient. Communities must also develop robust data back-up and recovery plans, keep all software up to date, and consider installing multiple, lower-level firewalls at all sites so an infection may be isolated before it spreads throughout the network. These strategies, implemented in concert, can lessen the effect and even prevent these increasingly common attacks.

A school's most precious resource is also its most difficult to recover: student data. When a student's private information is stolen from a school network, thieves can—among other crimes—use student identities to run up vast sums of credit card debt. Worse, because the theft may go undetected for many years, students may not know of their ruined credit until they hear from a debt collector or find their applications for student loans rejected. The consequences of such fraud may cripple a student for years.

Schools must therefore take every precaution to protect their students' data. In part, this responsibility means recognizing that there is no one-time fix for all security concerns; rather, schools must make an ongoing commitment to improving security and responding to new threats as they emerge. According to CoSN's Linette Attai, a good data security plan will include physical, technical, and administrative components, each of which should evolve with changing best practices.

4 Compromised Business Email

According to the FBI, over the past three years businesses have squandered more than $26 billion through compromised emails. These attacks take many forms, but in each a fraudulent email induces someone to send money to thieves. Sometimes the phishing scheme comes from a hacked account, sometimes from a phony supplier, sometimes from a fake attorney requesting privileged information. In each case, because no dangerous links are included in the email, it can sail right past many security solutions.

While there is no sure-fire protection against such schemes, ensuring that each network user is on the lookout for such emails and knows what to do when one is found can be a great help. Further, it is essential to establish community-specific protocols that indicate how and when sensitive information or funds are to be shared.

5 SQL Injections

SQL injections come in many forms, but all involve an attacker "injecting" an SQL into a database query. In these longstanding, but incessant attacks, once an injection is established on an unprotected database, attackers can issue their own commands. If unblocked, an attacker will be able to steal a network's most important data.

Fortunately, you can protect yourself against SQL injections. Not only is it essential to sanitize the information moving through your network, it's important to limit the privileges an application needs to run—that way you minimize your exposure to threat. As usual, due diligence about best practices will reduce your risk and keep you safe.

To discover how ENA's robust suite of security solutions can strengthen your district's cyber defenses, visit www.ena.com/security.

ABOUT ENA

ENA is the leading provider of technology solutions to education communities and libraries. Since 1996, we have worked with our customers to ensure they have the robust and reliable connectivity, communication, cloud, security, and software solutions they require to meet the present and emerging technology needs of the communities they serve. For more information, please visit **www.ena.com**, call **866-615-1101**, or email **info@ena.com**.