PROTECTING YOUR K12 NETWORK FROM TOTAL SHUTDOWN

As the number of news making corporate cyber-attacks increased over recent years, cybersecurity has become top of mind for professionals of varying industries. One way to prevent this activity from occurring is to protect yourself from the most common cause, DDoS.

A DDoS (Distributed Denial of Service) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. Recovery from these types of attacks can take anywhere from a few hours to a few weeks, and some systems are never fully restored to their original state.

WHY ARE SCHOOLS INCREASINGLY BECOMING A TARGET FOR ATTACKS?

Schools are typically vulnerable and unprepared for DDoS attacks.

Few schools can afford to have a full-time IT person on staff dedicated to network security.

Students may be interested in carrying out these attacks for personal benefit

Students and faculty are increasingly bringing their own laptops, phones, and other personal devices to campus and connecting to the campus network, bringing in increased risks for cyberattacks.

Schools rely on technology for day-to-day operations.

It doesn't necessarily take a sophisticated hacker to carry out a DDoS attack; students also have the knowledge and potential to breach the system.

A simple Google search can give a tech-savvy student the information they need to hack a school's network.

- A student can pay a hacker as little as **$20** on test day to bring down the system in order to get out of taking a test. To the student, it's not unlike pulling the fire alarm to get out of a test.
- As more required student testing is done through online networks, attacks designed to bring down online testing events have become increasingly problematic.
- Cyber criminals can use a DDoS attack as a smokescreen to access proprietary & financial information from school servers.
- It's relatively cheap and easy to hire a hacker to implement a DDoS aatack.

The cost of such an attack? Schools that experience this type of data breach could face consequences from reputation damage to loss of funding.

A TOTAL SHUTDOWN CAN RESULT IN ISSUES WITH

- Registering students
- Student testing
- Grading
- Controlling student absence
- Paying for school lunches
- Physical camera security functionality
- Performing administrative work
- Distributing educational content
- Student Safety
- Pursuing e-learning efforts

PROTECT YOUR NETWORK FROM TOTAL SHUTDOWN

DDoS attacks are not always easy to recognize, as they can be hard to differentiate from the normal ups and downs in network performance activity.

These recommendations can help to better protect your network from a cyber-attack & help your network to rebound more quickly should an attack occur.

CREATE A DEFENSE STRATEGY

The best offense is a good defense. **Develop an IT security policy with defined security protocols** that can be implemented school-wide. Having a detailed plan in place will help you mitigate potential damage.

Ensure that an incident response plan is in place *just in case an attack does occur.*

It's important that the faculty know the steps they need to take ahead of time in order to respond appropriately. Being proactive will help you rebound from an attack faster than if you ignore the potential for these types of threats.

Being proactive will help you rebound from an attack faster than if you ignored the potential for these types of threats.

Stay current with trends, signs, and patterns associated with DDoS. The more you know about them, the better prepared you'll be.

KEEP HARDWARE, SOFTWARE, & SECURITY SAFEGUARDS UP-TO-DATE

Even if you don't think you're at risk,it's imperative your security safeguards are up-to-date. This will help protect you against an attack and ensure your infrastructure is as secure as it can be

REMEMBER TO

- Use a Firewall for your internet connection
- Protect network passwords
- Download and install software updates as they become available
- Monitor your systems continuously to detect potential problems
- Install, use, and regularly update anti-malware, anti-virus, and anti-spyware software on every computer in your school
- Create a BYOD policy for students and staff to ensure they are securely connected to your network

Being proactive and implementing the recommendations above will not only help you prevent DDoS attacks, but other types of cyber-attacks as well.

EDUCATE STUDENTS & FACULTY

Everyone involved with the school needs to be mindful of the risks not only associated with the attacks, but also the consequences associated with carrying out this type of federal crime.

The more educated students are about the consequences, the less likely they'll be to implement an attack. The more educated teachers are about warning signs & patterns, the more likely they'll be to stop these attacks before they happen.

BRING IN THE EXPERTS

Schools that can afford to have an IT staff often find them consumed with the demands of day to day activities, electronic classrooms and making sure education-related systems are running appropriately. A DDoS attack can significantly impact these resources.

IF THIS IS THE CASE WITH YOUR SCHOOL...

Consider outsourcing the network security to an IT specialist or managed service provider who can focus all of their attention on it. While there are many IT specialists, consider working with one who has previous experience in the K-12 education system.

Your IT department, IT managed services provider, or Internet service provider may have resources for DDoS mitigation. If so, they may have the ability to detect DDoS attacks. and reroute traffic in the event an attack does happen.

HOW COX BUSINESS CAN HELP

If you are in a Cox Business serviceable area, contact us directly to find out more about our DDoS mitigation services.

COX Business®
www.coxbusiness.com/k12security
Education K-12 Assets - 1-866-743-1451