Education Cyber Security Guide

Cyber Security Challenges for Schools

Educators know that the Internet is a double-edged sword. While easy Internet access means students have a wealth of valuable information at their fingertips, the Internet also delivers material and unwanted agents that can harm both students and your school's networks.

Schools face many challenges with Internet access and the integration of technology as the norm in education, the exponential growth of Internet access and the integration of technology into education, from kindergarten through high school. The popularity of the 1:1 computing initiative and the challenges of bring your own device (BYOD), mean that school IT professionals are faced with protecting students and networks from a wide range of emerging Internet threats. Also, CIPA and other regulatory requirements demand that schools safeguard students from inappropriate content and protect both students and staff from the exposure of confidential information.

Social media sites , such as Facebook, Twitter, and YouTube, have changed the landscape of education forever. Your schools ability to protect students, maintain regulatory compliance and protect the schools' networks depends on having the right technology in place. EdgeWave security solutions including iPrism Web Security, originally created for schools, and the ePrism Email Security Suite offer the ideal combination of features and functionality that can protect your students, while helping support an enriched learning environment that uses the valuable tools the Web has to offer, while mitigating threats.

Social Media and Cyberbullying

Even in 2016, cyberbullying continues to be one of the biggest challenges facing schools as they try to create an atmosphere of social networking security for students is to understand how cyberbullying is manifesting itself in their schools. Because attacks can occur quickly and anonymously and spread rapidly, cyberbullying can cause significant damage to the students who are the subject of such attacks. It negatively impacts the self-esteem of its victims and has even led to physical damage and distress in students. While most states have passed both anti-bullying laws and policies, schools are expected to be more vigilant. Schools don't merely block social media applications, but administrators now have visibility into students' online activities.

Digitization

Schools have been radically transformed by digital technology – smart phones, tablets, and web-enabled devices have altered how schools deliver education. At the same time, technology has enabled a new generation of risks and threats, from unauthorized access to the network to stolen student records. Data breach prevention has become increasingly important.

Congress moved to protect students and schools with the Child Internet Protection Act (CIPA), passed in 1999. CIPA was created and tied to E-rate funds in order to induce elementary and secondary schools and libraries to take measures to filter and block unwanted Internet content from reaching students. The E-rate program helps schools and libraries pay for products and services such as Internet access, internal network connections and telecommunications and are an important funding adjunct to school budgets. Every school is aware of CIPA requirements and most have deployed deployed a Web filter per this legislation's mandate. However, students' success in circumventing many filters by using anonymous browsing sites or non-sanctioned protocols can open schools to non-compliance and a loss of important e-rate funds.

HIPAA Compliance

Schools are now aware that they are also subject to HIPAA compliance. The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996 in response to several issues facing health care coverage, privacy, security, and fraud in the United States. And because schools keep health records and may have healthcare workers on-site, such as a school nurse, they are in effect performing or assisting in the performance of an activity or function that involves the disclosure of protected health information. Violations can happen in a school settings when protected health information about students or staff is sent from the school. Failure to comply with HIPAA regulations can result in severe fines and schools that are lax in this regard could be open to litigation.

Education Cyber Security Guide

iPrism Defends Against Internet-Based Threats

The Web is replete with threats that can cause direct and collateral damage to your school including the risk of non-compliance. The exposure of private student information via hacker exploits can have serious consequence including non-compliance fines and convictions, lawsuits, network damage, student access to inappropriate content and more. iPrism Web Security, the secure Web gateway originally designed for schools, offers the features and functionality you need to protect your students and networks from current and emerging web-based threats.

iPrism Circumvention Defenses - Circumvention techniques are becoming more sophisticated every day and easily accessible to your students. iPrism's blocks attempts by circumvention tools to connect, rendering them harmless and protecting your school from opening the network to criminal malware designed to steal data. Once the circumvention threat has been blocked, iPrism's Email Alerts and Real-Time Monitor features can be used to address the transgressors and take more serious action if required.

iPrism Botnet Technology – Bots are autonomous applications created for financial gain that can infect networks by being joined together into huge networks called botnets. Botnets can do massive damage before they are detected. iPrism Web Security leverages a comprehensive botnet threat index to prevent bots from phoning home and forming botnets. Once a bot has been detected and blocked, users are alerted via email and Real-Time Monitor so they can remediate compromised endpoints, knowing that the immediate threat has been mitigated.

Real Time Monitoring and Reporting - iPrism on-box reporting will show compliance with regulations that protect users' identities and data.

More Defense with Application Controls - iPrism allows you to monitor and block IM and P2P applications such as Skype and FTP with a simple set-and-forget check box.

ePrism Defends Against Email-Based Threats

Email is another access point that if not secured can undermine your efforts to stay compliant. Unfortunately, the technologies that make data easy to access and share also increase the risk of unauthorized disclosure and loss of sensitive, protected data. EdgeWave's ePrism Email Security Suite includes the powerful tools you need to assure the protection of private data of your students and staff and the efficient delivery of legitimate mission-critical email. ePrism offers fully hosted in-the-cloud services that require minimal management, are affordable on tight school budgets and can scale easily to fit any size school or district.

The ePrism Email Security Suite includes:

Email Filtering – ePrism email security includes a multi-layered approach that stops emerging threats before they can get near your network. Our exclusive Zero-Minute Defense incorporates real-time, session-level defenses against malware such as botnets, by employing a system that is automatic, adaptive and behaviorally-based. Our ability to keep these threats out of your email also conserves bandwidth, keeps mailboxes uncluttered, and because they are behaviorally based and key off the botnets' known sending characteristics, virtually eliminates false-positives. The result is more efficiency and faster delivery of legitimate email.

Email Continuity – Email has become an indispensable tool in the normal functioning of almost all organizations, including schools and even a short period of downtime can have serious consequences. ePrism Continuity enables continuous web-based email access, management, and use during planned or unplanned mail server outages. This service is enabled easily via a simple admin check box, giving your users access to their mail so that they can manage messaging and avoid any disruption in the flow of important communications. In case of an outage, end users access the Web email client allowing them to read, compose, reply to, forward and delete messages and upload and download attachments, as though no interruption had occurred.

Data Protection Services

- **Data Loss Protection** - This service includes a content analysis and policy engine that uses proprietary technology to detect private information transmitted via outgoing email. This data protection technology analyzes data in motion and using compliance based rules, detects and blocks any sensitive private data trying to leave your network. This solution is easily managed from the ePrism Central Dashboard giving you the powerful tools you need to comply with government regulations such as HIPAA and others.
- **Encryption** - EdgeWave Email encryption assures the secure delivery of email to anyone outside your school or district, with next-generation technology that eliminates the cost and complexity associated with many traditional encryption services. As a completely hosted service, there is no hardware or software to implement and encryption can be easily enabled on a per

user basis or as part of an automated routing policy. In addition, because it is integrated into the ePrism Hosted Email Security and Data Loss Protection services, your outgoing email is inspected for malware, viruses, inappropriate content, compliance breaches and violations of your school's acceptable use policy (AUP) – a more multi-layered defense than a solo encryption service can offer. You can manually encrypt messages or configure it to automatically encrypt per a variety of factors such as sender, recipient or when DLP problems are detected.

- **Secure Archive** – ePrism offers secure email archiving that retains your schools email in an unalterable state to help you meet regulatory compliance requirements, possible litigation issues, or storage management needs. As a cloud-based solution, you are assured scalability and easy retrieval whenever you need to access a message. ePrism's secure data collection technology provides comprehensive interoperability with all messaging systems

Web and Email Security Solutions Feature Details - Ideal for Schools

iPrism Web Security Features

- **Easy-to-Use Technology** - Low TCO – iPrism, the Internet filtering appliance originally designed for schools, provides the lowcost, low-maintenance solution that meets your requirements for accurate and secure filtering while helping you maintain regulatory compliance. In two independent studies, iPrism was found to have the lowest total cost of ownership and lowest total cost of acquisition compared to leading competitors.
- **Maintenance-free, Self-Contained Solution** - iPrism requires no additional hardware or software and one low acquisition price includes everything needed for accurate monitoring, filtering and reporting. Once iPrism is up and running, it operates virtually maintenance-free. iPrism receives automatic database updates every night and in the case of critical security categories, updates can arrive hourly.
- **Enhanced Directory Integration** - iPrism authentication incurs no OS conflicts and integrates seamlessly with all major network directories including Novell Netware Directory Services (NDS), Windows Active Directory (including one-way outgoing trust support) for Window 7 and also Mac clients using AD 2003/2008 and Mac OSX Snow Leopard. In addition, as an LDAP variant, it is possible to integrate iPrism Web Filter with OSX Server Open Directory (LDAP v2/v3).
- **Hybrid Remote Filtering** - iPrism's new Remote Filtering delivers powerful Web security to your remote users without using your VPN and without adding any hardware in your DMZ or requiring browser-specific PAC files
- **Granular Policy Rules** - iPrism's convenient central management console lets you create different groups and give them different levels of access, helping you create an environment where teachers, elementary students, high school or college-age students can have different access levels while assuring the safety of each audience and the security of your network.
- **Comprehensive Logging, Real-Time Monitoring and Reporting On-Box** - iPrism's comprehensive on-box reporting requires no additional hardware or software and includes real-time monitoring and email alerts that give you highly accurate and timely visibility on Internet activity across your school. Reports can be flexibly scheduled and generated using a variety of templates or customized to suit your requirements. Email alerts are generated when security problems are detected allowing you to quickly mitigate threats before they cause damage.
- **US-Based Technical Support Services** – EdgeWave offers excellent technical support that consistently receives 94%+ ratings in customer satisfaction surveys. Calls are answered immediately with product experts on hand to resolve any issues.

ePrism Email Security Suite Features

- **Infinite Scalability** – No-Touch Email Protection - We host the applications and infrastructure required to protect your organization from the risks and threats of email processes including spam, malware, phishing, viruses, and inappropriate content. ePrism's comprehensive services also enable data loss protection, email retention, disaster recovery, and secure email delivery.
- **Proven Expertise** - We provide the technology expertise and front line defense required to fight emerging threats and risks so you can focus on growing your business.
- **Easy Set-up and Zero Maintenance** - You can be setup within inutes to start protecting your networks and data, all that's required is a simple MX path redirect. ePrism assures nothing to install and zero maintenance - the ultimate in a no-touch solution that conserves your resources.

- **Infinite Scalability** – ePrism Hosted Services scale to fit any size school and can grow with you if your student and staff population increases.
- **Bandwidth Savings** - Eliminating the volume of spam hitting your servers increases your available bandwidth for other internetbased applications. EdgeWave helps reduce bandwidth costs, as well as lessen the burden on your email servers' archive capacity.
- **Proactive Technical Support** - EdgeWave's Security Operations Center is staffed around the clock with email experts and security specialists to handle your support needs. They provide proactive monitoring of any email threats to assure continuous service for all EdgeWave domains and users

EdgeWave's award winning solutions have helped thousands of schools to protect their students and data as well as meet regulatory compliance and policies. Let us create and implement your school's cybersecurity strategy and protect you and your data today by requesting one of our representatives to contact you.

To learn more about EdgeWave and its powerful solutions, please visit https://www.edgewave.com/.

4225 Executive Sq, Ste 1600,
La Jolla, CA 92037

Give us a call:
1-800-782-3762

Send us an email:
info@edgewave.com

For more info, visit us at:
www.edgewave.com