



What *Every* Administrator Needs to Know About Cyber Security

Introduction: This guide provides school administrators with practical suggestions and resources for ensuring that computer networks are secure from cyber attacks. Every administrator in a school environment has an obligation to be knowledgeable about cyber security, including district-level administrators, such as superintendents, community directors and finance managers, as well as school-level administrators, such as principals, guidance counselors and libraries. Safeguarding computers in the schools is not just for technology professionals: it is every administrator's responsibility. While most school districts have security measures in place to ensure computer network protection, responsible administrators must guarantee that these systems are as secure as possible so that:

- Student and staff data remain private
- School technology property is not damaged from attacks from email viruses, inquisitive student "hackers" or malicious external infiltration
- Students, teachers and district staff have access to online information and network services through secure Internet and network connections.

Remember, secure computer networks benefit **EVERYONE** in a school community, and, likewise, a compromised or "hacked" network can prove very damaging. School administrators must take responsibility for making sure they understand the issues involved in securing computer networks and electronic data. Talk to your technology team and find out if your school district is "cyber secure." Make computer and network maintenance a top priority by working with your district technology team and school district community to ensure that everyone understands their role in securing education data.

Computer technology is a great tool in education: it helps administrators streamline decision-making, communicate with the education community, and provides multiple education opportunities for students and educators. However, these benefits come hand-in-hand with responsibilities for everyone in the school community. As school leaders and managers, District Administrators must make sure that computer network security is a top priority so that this significant resource investment is protected from outside – or inside – attack and misuse.

About NetDay: NetDay's mission is to connect every child to a brighter future by helping educators meet educational goals through the effective use of technology. NetDay (www.NetDay.org), a national non-profit organization known for its successful school wiring programs, today manages community and web-based programs that promote enhanced student achievement through the effective use of technology.



NetDay Cyber Security Kit for Schools *What Every Administrator Needs to Know About Cyber Security*

Cyber Security Guidelines For Administrators

Get Up to Speed on Network Security

Talk to your technology team and find out what security measures your school district has in place for your computer networks. Every district should have:

1. **Anti-Virus Software** – Every computer and server in your network should be protected with anti-virus software. Anti-virus software protects computers from viruses that destroy data and require costly repairs to computer systems. For optimal use, anti-virus software should be scanning all documents on a computer, as well as all incoming emails, on a daily basis. You should also check to make sure that your anti-virus software is downloading the most current virus definitions on a weekly basis. This ensures that your computer network is protected from the new viruses or “bugs” that are circulating through the Internet.
2. **Firewall Protection** – A firewall is software or hardware designed to block hackers from accessing your computer network. Firewalls are designed to prevent hackers from getting into programs and files. A firewall is different from anti-virus protection in that it makes a computer network invisible on the Internet and blocks communications from unauthorized sources.
3. **Data Backup** – Backing up system data and storing it offsite is an integral part of any cyber security plan. Regular data backups protect organizations in the event of hardware failure or accidental deletions, and also protect staff against unauthorized or accidental changes made to file contents. District administrators need to make sure that data backup is appropriate for the size and scope of the district’s network, and that backup files are created at appropriate intervals and themselves are well protected from damage and destruction in an off-site location.

Keep Confidential Data Secure

Over the years, school districts have established strict guidelines for storing paper copies of confidential student and staff data; in fact, local, state and federal laws require that these records be protected from unauthorized release. As districts begin to store confidential data electronically, these same laws apply – so electronic data security should be a top priority for administrators.

1. **Network Security** – The guidelines and recommendation above are a very big part of keeping district information secure from inappropriate external access or internal hacking.
2. **Protocol for Accessing Network Information** – Ask your technology team about their protocol for establishing user access to network data. For example, a school principal should have access to more data resources on a network than a 6th grade student. Ask for an overview of the rules and regulations that govern how a user accesses the network. For example, is district and school staff allowed remote access to the network? Ask how often users are required to change network passwords.



NetDay Cyber Security Kit for Schools *What Every Administrator Needs to Know About Cyber Security*

(Continued: Cyber Security Guidelines For Administrators)

3. **Establish Guidelines for Electronic Communication** – It is very easy to send an email to the wrong person, or to send the right person the wrong attachment. These types of mistakes are usually harmless, but it is important for a school district to establish electronic communication guidelines when private data are concerned; for example, if files should be encrypted before they are distributed electronically.

Establish Bi-Yearly “Network Security Checks”

Work with your district technology team to establish regular “security checks” each year to ensure that you are keeping up with the latest advances in network and computer security. For example, a school or school district may establish a “security check” at the beginning of each semester. Stay Safe Online (www.StaySafeOnline.info) offers additional resources and information to help keep school administrators and technology staff up-to-date on the latest developments in network and data security.

Educate the School Community about Cyber Security

The entire school community contributes to the district’s network security. District and school staff, teachers, students and parents should know how to protect themselves and their personal data from attack.

1. **Passwords** – Setup a district or school plan for proper password maintenance and security. The golden rules of passwords are:
 - a. A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters and numbers, e.g., xk28LP97.
 - b. Change passwords regularly, at least every 90 days.
 - c. Do not give out your password to anyone!
2. **Email** – Email is one of the most popular online communication tools for both children and adults. It is also the easiest way to spread email viruses that can damage computers and computer data. Both children and adults should only open emails from people they know. If an email address is unfamiliar, they should delete the email without reading the message. If an email with an attachment is received, the recipient should be sure to verify that the attachment is safe and virus-free before opening it. Just to be safe, email attachments should only be opened if the recipient knows the sender and is expecting to receive an email with an attached file.
3. **Online Chat** – Online chat rooms are popular destinations for some children and adults. Be sure that parents and teachers monitor Internet use closely to ensure that children are accessing age-appropriate web sites. Be careful about providing too much personal information in a chat room...remember, a chat room is a public space, and you never know who is actually visiting this virtual space.



NetDay Cyber Security Kit for Schools *What Every Administrator Needs to Know About Cyber Security*

(Continued: Cyber Security Guidelines For Administrators)

4. **Instant Messaging** – Instant messaging, which is similar to “real-time” email, is a great way to increase productivity while connecting with friends, family and colleagues. However, users should be careful about communicating only with people they know, and also recognizing that viruses can be spread through instant messaging just as easily as they can through email.

Establish and Enforce Technology Use Guidelines

Establish and enforce proper use policies so that the entire school community understands proper computer etiquette and use in the education environment. These policies should set clear guidelines and repercussions in the case of abuse. Schools should make every effort to communicate these guidelines to teachers, children, parents, and others impacted by these policies. For tips on developing an acceptable use policy, visit Classroom Connect’s Hints and How-Tos at <http://www.connectedteacher.com/tips/aup.asp>.

Additional Resources for Administrators

The resources listed below have been reviewed by NetDay’s editorial team and are part of NetDay’s award-winning web site, www.NetDayCompass.org.

1. **Safeguarding Your Technology** - This guide has been developed specifically for educational administrators at the building, campus, district, system, and state levels (e.g., school principals, district superintendents, state chiefs, college deans, and their assistants). It is meant to serve as framework for understanding why and how to effectively secure an organization's information, software, and computer and networking equipment.
<http://nces.ed.gov/pubs98/safetech/>
2. **Scholastic Administrator: Policing Your Computer Networks** - This article from the Spring 2002 issue of Scholastic Administrator Magazine details how to protect a district’s technology assets from hackers, Internet worms and computer viruses.
<http://www.scholastic.com/administrator/spring02/features.asp?article=policing>
3. **The Cybercitizen Partnership** - The Cybercitizen Awareness Program educates children and young adults on the dangers and consequences of cyber crime. By reaching out to parents and teachers, the program is designed to establish a broad sense of responsibility and community in an effort to develop in young people smart, ethical, and socially conscious online behavior.
<http://www.cybercitizenship.org/>