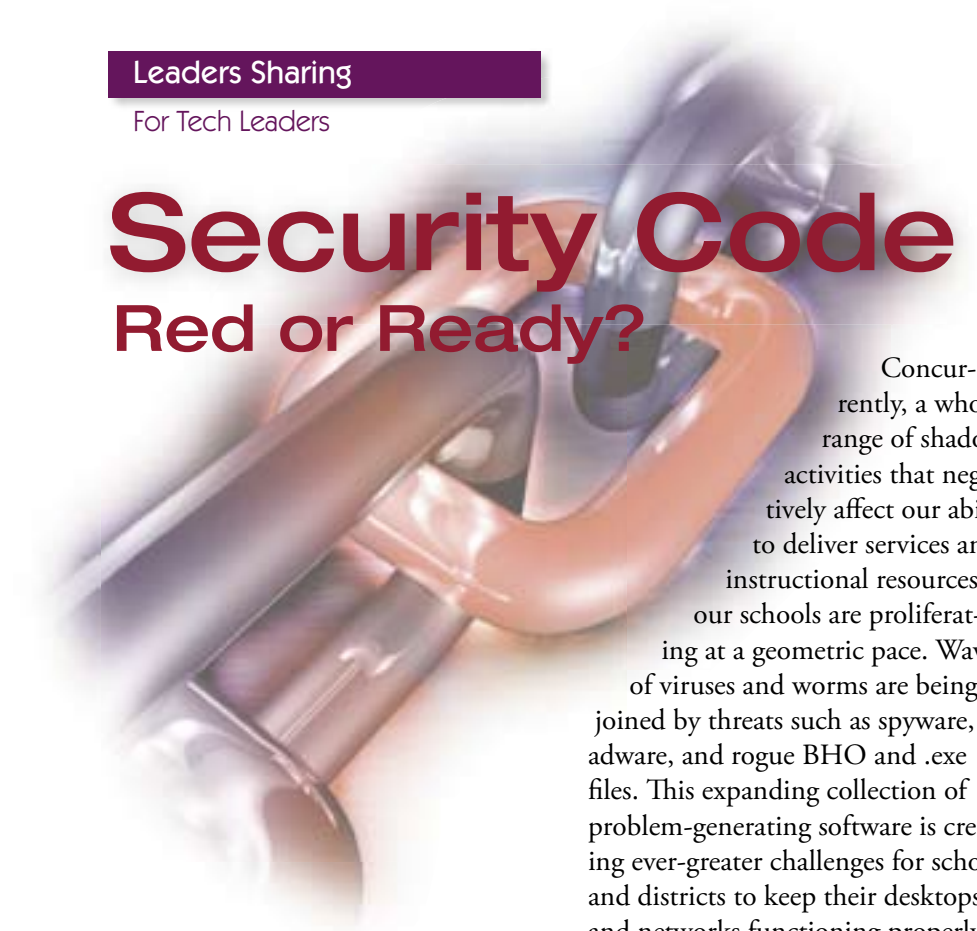
Security Code
Red or Ready?



Increasingly, teachers rely on computer software and networks to both enhance curriculum management and provide engaging learning opportunities in instruction. New software is enabling more frequent formative assessments to better focus day-to-day lessons on the unique needs of individual learners. Administrators use increasingly complex data management systems to assess students' progress (individually and aggregated) and make data-based decisions to improve student achievement. Together, they are developing school improvement plans to help students achieve mastery of academic standards as their schools face the growing call for even greater accountability at local, state, and national levels.

By Don Hall and Pat Kelly

Subject: Network and data security

Standards: *NETS•S* 3; *NETS•A* IV (http://www.iste.org/nets/)

Concurrently, a whole range of shadow activities that negatively affect our ability to deliver services and instructional resources to our schools are proliferating at a geometric pace. Waves of viruses and worms are being joined by threats such as spyware, adware, and rogue BHO and .exe files. This expanding collection of problem-generating software is creating ever-greater challenges for schools and districts to keep their desktops and networks functioning properly. The cyber-nasties have made a dangerous place of our gleaming fiber, DSL, and T1 lines.

Fortunately, strategies to combat these new attack agents are becoming flexible and intuitive. Newer software enables us to schedule automatic updates, and central office virus servers can push out needed updates during non-school hours. Web-updated software and data encryption schemes have improved our defenses against attacks. Yet we all need to become educated volunteers for electronic defense if we are to hold the line against downtime and compromised data. In this article, we look at the electronic security challenges facing schools today as well as practical steps they can take to address them.

Where Do I Start?

Although it's difficult not to sound like you're working for the network security police, many no-cost practices can help improve the security and reliability of your network. Beyond the obvious solutions of installing virus protection, firewalls, and filtering software, our most effective defense is the education of our user community. As one sage once said, "If you are not part of the solution, you are part of the problem."

Model appropriate behaviors and set high expectations for compliance with your school district's Acceptable Use Policy (AUP). One way of doing this is to review the AUP with all staff and students annually. This includes noninstructional staff. Experience demonstrates that most staff-level abuse occurs before and after the official school day.

Student abuse most often occurs when they are unsupervised. So be aware of where and when you provide the greatest level of unsupervised access to technology in your school.

Avoid shared, generic network logins. To foster greater accountability and assist in rapid problem resolution, the use of personalized staff and student network logins should be standard. It is important to know which student or staff member is using each computer connected to the network.

You also have to determine what level is practical. For example, it may not be viable to have your kindergarten students have unique student logins and passwords, but the risk level is much lower as well.

Staff should not leave their computers logged in to the network when they leave the immediate area, even for a few minutes. Staff members need to be reminded that as long as they are logged in to their machine, it appears that anything sent from that

computer is from them—good or bad. Also it can provide opportunities to access they did not plan for. Unfortunately speaking from experience on this issue, that is all it takes for a savvy student to install spyware on your PC.

Our high school students often assist guidance counselors, among others, with technology issues. On one occasion, a student installed spyware on Monday and collected all the keyboard entries through Tuesday and Wednesday, then downloaded the collected information to disk at the next opportunity. Later, at home, he was able to ascertain the counselor's desktop password, log in to the system, and begin altering grades and attendance records. Unfortunately for this student, in our district, the net result was an automatic 3–5 day suspension and loss of access rights to any system resources, including the Internet, for up to a year.

Allow only district standard devices to be connected to the network. Support your building-level computer coordinator by only allowing connection of devices (e.g., hubs, routers, Web or surveillance cameras, wireless access points) meeting your district's approved hardware standards. This is important for a number of reasons.

It makes technical support much easier; therefore, you are more likely to have a functioning and supportable technology program in your building. Additionally, you are less likely to introduce external threats or risks into your environment that could transmit viruses or contaminate your network.

Usually district-standard equipment has been tested for compatibility and interoperability, which cannot always be said for personal equipment or local choice options. This should reduce the overall chance of it crashing your network.

Exercise caution and investigate carefully when implementing any communication strategy permitting indirect connection to your network. Schools are looking to increase the level of access to their data for staff and students as well as the community. However, this increases the level of risk and complexity. Therefore, you must understand the options more fully and consider the implications of each before adopting them and opening your network up to outside influence.

Do not install any modems without coordinating with your central technology support group. Modems present a significant security risk. They are like putting in another door for outsiders to enter your system.

Only install wireless access points using secure encryption. Keep your operating system, Web browser, and desktop antivirus software up to date.

If your students are on the net, your teachers should be on their feet—monitoring. Under no circumstance should a student be allowed to access a computer on the administrative network using a staff account.

Only allow licensed and authorized software on your school's PCs. Physically isolate your server in a secure location, and limit access to only those staff who manage the network.

May I Have the Keys Please?

Another way we can make our network and data more secure is the area of password management. One of the easiest policies to establish but most difficult to enforce is to insist your staff maintain the integrity of their user login and password(s). Many staff members fail to realize the power of their password or the responsibility that goes with it.

I often ask my teachers, "Would you drive some of your most troubled students to your home, hand them the keys to your front door, leave them there alone, and then go to the mall for the day?" I don't think so. Yet we do that regularly when it comes to our electronic keys.

Some basic guidelines will help you and your staff make this process less painful but still establish a solid line of defense. Passwords should be secure but easy to remember. Avoid guessable passwords and change them often, particularly those you are using on the Web.

Password Do's. Make your password at least eight characters long with at least one number or symbol. The number or symbol should not be at the beginning or end of your password. Change your password regularly and don't write it down. Most potential hackers know to look under the keyboard and mousepad. That's as senseless as hiding the door key under the doormat.

Use longer passwords; they are more difficult to crack or guess and mix upper- and lowercase letters in your password with punctuation symbols. Combine two short words with a symbol (e.g., low@carb).

Use the first letters of an easily remembered sentence or line from a song, for example, "Get Me to the Church on Time"—GmttCoT or "On the Street Where You Live"—OtSWYL. Okay, so now you know I like Lerner and Lowe and figure you could guess my passwords. Not so; next month my passwords may be based on Herr Mozart's greatest hits. Remember, change your passwords

often. The best defense is a good offense.

Password Don'ts. Don't use "password," "secret," your school mascot, initials, birthday, phone number, home address, song or book titles, musicians, vocalists, family or pet names, make and model of your car, or your favorite beverage. If the hacker knows anything about you, then they will know about your password.

Don't use acronyms, reverse keyboard sequences, nor substitution schemes. Even the youngest "Sherlock" in your school will try these. Don't use the option on your computer or a Web site to remember your password for you. Anyone else using your PC would also have access.

Anytime you change your password, don't keep the same password and simply add a number to the beginning or end of it. For example, TheIsland and next month it is TheIsland2.

I've Been Hacked—Now What?

For most people, if they follow the guidelines we've already outlined you should not have to worry about this concern. However sometimes, even the best-laid plans can go astray and you find yourself on the wrong end of the hacker's attack. So what do you do when you know you have been the target of a successful attack? Contain the effects.

Key Steps for Containment. Call your technology help desk immediately and report the problem to them with as much detail as you can. Disconnect infected computers from the network but do not shut them down. Unplug any modems from the telephone jack.

Preserve any evidence of the attack. Write down time, date, and any messages on the monitor screen, and don't let anyone else touch the PC until your technology services staff arrive. Do not let anyone remove any other equipment such as flash drives and disks that are in the computer or in the immediate vicinity.

Have any staff involved document what they saw, heard, or did just prior to the problem.

Summary

As educational leaders, we need to keep our virtual learning environments safe and secure just like we do our physical learning spaces. Yes the dangers are real. We need to protect ourselves and our districts from liability for copyright infringement. We need to prevent unauthorized access to student records and sensitive personnel data to comply with Health Insurance Portability/Accountability Act (HIPPA) and Family Education Rights and Privacy Act (FERPA) regulations. We need to protect the significant investment our communities have entrusted us with in terms of technology equipment and software. Most important, we need to protect our students from the slightest possibilities of harm through unwanted or inappropriate contact with individuals or content.

Although we cannot control the types of electronic threats that exist outside our schools and districts, we can take proactive measures to ensure our children, data, and technology resources are safe. We can also make sure the data and technology resources are available to support instruction and school management. Sometimes those steps are through providing additional technology-based solutions. However, the most effective protection is an educated staff who realize the power, potential and responsibility they have for being part of the solution. Our goal is to ensure positive outcomes, not just protect ourselves from negative ones.

Don Hall is the executive director for information technology with the Kent (Washington) School District. He is the volunteer editor of L&L*'s For Tech Leaders column. He's a career educator with more than 15 years' experience in teaching and administration. He has also previously held senior leadership roles with General Electric and the Kentucky Department of Education, Frankfort. Don is a veteran conference presenter at the national and international level, published author, and experienced consultant.*

Pat Kelly is the executive director of technology services for Frederick County (Maryland) Public Schools and CEO of Trinity Enterprises, an educational technology consulting corporation. He has more than 20 years of central office responsibility for information technology planning and implementation in support of both instructional and operational objectives.