One of the challenges teachers face in a small school is the need to "spread themselves thinly" over areas in which they have little experience or expertise. This is especially true when it comes to maintaining computer security. This article provides some advice for teachers in this situation. It includes topics such as maintaining physical security, keeping important files safe and away from prying eyes, protecting students from dangers on the Internet, providing protection from malicious software, and finding sources of support.

COMPUTER SECURITY FOR SMALL SCHOOLS

BY PETER WALLACE

Physical Security

Physical security requires a little knowledge and a lot of common sense. Here are some specific problems to avoid:

1. Temperature extremes. Computers produce heat, so their ventilation holes need to be kept open to maintain air flow. Placing a laptop on a soft surface such as a bed can block ventilation and lead to overheating. Very cold conditions also pose a risk, usually from condensation.

2. Moisture and other liquids. Water can conduct electricity, so all types of electrical equipment must be kept dry to prevent shock hazards. However, even small amounts of liquid can damage electronic equipment. If equipment does become wet, it should be switched off until dry. Placing the item in a dry, warm place may prevent damage if only small amounts of clean water were involved. Unfortunately, this is not the case when juice or beverages find their way into computer components. To clean the mess, it may be necessary to pay a technician to dismantle components and possibly replace parts.

3. Physical damage. Most computer equipment is fragile. Monitors, hard drives and CD/DVD drives are particularly vulnerable to severe vibration, which is not usually covered by warranty. Drives are more vulnerable while running than when they are switched off.

When shopping for electronic equipment, try to buy items that are sturdy and "childproof."

4. Power surges and spikes. This risk is often greater in rural areas than in cities. A surge protector protects equipment from moderate surges and is a good investment. It is also wise to switch off electronic equipment at the end of the school day and when an electrical storm is approaching.

Modems are quite vulnerable to spikes through the telephone line. Unplug the phone line or high-speed Internet connection when storms pose a threat.

5. Dust. Floppy disks, CDs, and DVDs are vulnerable to damage from dust. A build-up of dust inside computers can lead to overheating, so keep off the floor and away from windows. As computers age, check inside the case for dust accumulation. You can remove the dust with a narrow vacuum cleaner attachment, but take care not to get too close to components, or you might suck them out with the dust.

Physical security also includes some precautions that can easily be overlooked:

1. Keep warranty documents and manuals where they can be found easily.

2. Keep track of purchased software, original CDs, and licenses. Many schools give this responsibility to the librarian, but administrators and teachers still need to be aware of licensing conditions and copyright laws (see Janine Lim's article on copyright restrictions in a previous issue of this journal: http://circle.adventist.org/browse/resource.phtml?leaf=5180).

Data Security

Data security refers to keeping important information safe. This includes preventing documents from being lost or corrupted and ensuring that sensitive information is accessible only to authorized personnel. The value of the documents will determine the precautions necessary to maintain data security.

Some of the threats to data security include the following:

1. Forgetting where a document was saved.

2. Accidentally deleting files or saving another document with the same name, thus deleting the original.

3. Leaving a disk or portable drive where it can be taken by people who should not have access to it.

4. Leaving a computer logged in and unattended, thus allowing unauthorized people access to it.

When shopping for electronic equipment, try to buy items that are sturdy and "childproof."

5. Careless treatment of passwords, failure to use a password, or using one that is easy to guess.

6. File corruption, which makes files unreadable.

7. Failure, loss, or theft of computer equipment.

8. Deliberate action by people wishing to cause harm. This can range from mischievous children to hard-core hackers. Maintaining data security requires both a planned backup scheme and careful measures for access control.

Organization

Document loss often results from poor organization. Some teachers who maintain a very systematic filing cabinet seem totally disorganized when saving files on their computer. Organization requires the creation of a folder structure and logical naming of folders and documents so that everything is saved in a way that makes it easy to find. In the "old days," when DOS was the main operating system, people had to use short, cryptic file names. This is no longer necessary, so use filenames that will still make sense to you in a few years.

Backup Methods

Depending on the size of the school's computer network, a backup scheme may need to be complex or simple, and can be manual or automated. Here are some low-cost options suitable for small schools:

1. Copying files to floppy disks. Floppy disks can be quite unreliable, so this option is not recommended.

2. Copying files to CDs or DVDs. CDs and DVDs are reliable, have much greater capacity than floppy disks, and provide a good option for archival storage.

3. Copying files to Flash drives. Flash drives, also called USB drives, are fast, reliable, convenient, and quite tough. They provide an excellent option for short-term backup.

4. Copying files to portable hard drives. Portable hard drives connect to a computer via a USB cable. They function like Flash drives but have a much greater capacity. They provide an excellent option for daily backup. However, schools should have two such drives. One should be kept in the safe while the other is in use, then they can be swapped the next day.

5. Sending files to an e-mail account. Hotmail, Yahoo, and GMail provide free e-mail addresses with plenty of free space. If you have good Internet access, this provides a free alternative for files that do not contain sensitive data.

6. Copying files through a network to another computer. Copying files to a preferred backup destination is a simple task, but ensuring that users have the latest version of files can be time consuming. Synchronization software (such as the Synchronization feature in Windows XP) makes this task a lot easier. It can automatically copy everything new from the computer's documents folder to the portable hard drive and replace old versions. Synchronization software can also be used to synchronize files with other computers on the network.

Planning a Backup Scheme

Whatever methods you choose, the procedures need to be systematic and regular. Choose what to include in your backup scheme, including all documents produced in the principal's office and by teachers, student data, academic records, financial records, personnel information on aides and volunteers, and library records. Documents produced by students and stored at school should also be included.

If your school uses digital cameras, exclude photographs and movie files from the normal daily backup since the quantity of data may dramatically slow down the backup process. Copy these large files to DVDs.

You should consistently use three methods of backup: day-to-day, off-site, and archival backup. Be sure to label CDs and other removable media so that you can identify their content and backup date.

1. Make backups every school day.

2. Store backups in a safe, waterproof location. At school, the safe or strong room would be the best.

3. Use two different backup methods. For example, store materials on portable hard drives, and send copies of files to your GMail account.

4. In addition to backups stored at school, maintain off-site backup so that if your safe and computers are stolen, destroyed, or damaged, this valuable data can still be recovered. Taking an additional copy of your backup home may be satisfactory as long as you have a secure place to store it.

5. Try to automate the backup procedure. Server operating systems and most synchronization software can do this.

6. At regular intervals, make an archival backup of all office and teacher files and a separate backup of student files.

Archival backups could be done at the end of each term and before computers are upgraded. Archival backups are usually stored on CDs or DVDs, but make sure they are stored securely and systematically for quick retrieval.

7. Be sure to review and test your backup procedures on a regular basis to ensure that procedures are working as expected.

Access Control

Breaches in access control can be damaging and embarrassing. Allowing confidential information to become public could lead to litigation. Here are some safeguards:

1. Choose secure passwords. A combination of numbers and letters with a total of at least eight characters (including several that use the shift key) is recommended.

2. Keep passwords secret. Breaches of security could result from students' overhearing passwords or seeing a password written.

3. Log off or lock the computer before leaving it. In Windows XP, locking is as quick as holding the Windows key and pressing L. Unlocking requires your password.

4. Ensure that each user has a secure documents folder.

5. Do not allow students to use the login of a teacher or computer administrator.

Create a separate account for each student. (This is also an important precaution to employ on the teachers' home computers.)

6. Be careful where you leave disks, CDs, and portable drives.

7. If you use a file server on your network, ensure that staff and student data is stored in different partitions and that students are not allowed to access the staff partition.

8. Be especially vigilant about the security of files containing sensitive information such as Social Security numbers, grades, personnel matters, and financial information.

Even small amounts of liquid can damage electronic equipment.

9. When redeploying or disposing of computers, ensure that all sensitive data is erased from the hard drive.

Protection Against Malicious Software

Viruses, worms, trojans, and spyware pose a continuous threat to computers, particularly those that can access the Internet. The term *virus* is often used in the generic sense to include worms and trojans. Because viruses can spread so quickly, it is best to have anti-virus and anti-spyware software configured to update automatically using reliable sites on the Internet. Computers that are not connected to the Internet should still be updated regularly because many viruses can be transferred by files on disks or other removable media.

In addition to software protection, it is essential to educate both teachers and students to use safe practices which include the following points:

1. Do not open e-mail attachments unless they have been checked by anti-virus software, you know who sent them, and the message of the e-mail is consistent with your knowledge of the sender. Those who distribute viruses are very cunning and increasingly rely

on deception as much as on technology.

2. Be wary of links in e-mail from unknown sources. Never click on links in spam messages.

3. Never reply to spam messages, or those that ask for personal information or financial data. Warn students not to reveal information about themselves in chat rooms or in response to e-mail inquiries.

4. Be very careful about downloading programs from the Internet. Software from reputable sources is unlikely to contain viruses, but determining which software and download sites are reputable will require some research. A series of Google searches using the names of the software and the site, along with the word *review*, will allow you to read what reviewers have written.

5. Avoid clicking on pop-up messages, which can deceive you into installing malicious software. If in doubt, do some research on Google using the terms from the popup message.

Software Updates and Patches

Modern operating systems are very complex and contain millions of lines of code. Errors in the code can be exploited by hackers, so software manufacturers release periodic updates to fix these errors. As soon as an update is released, some hackers analyze the update and write malicious software to exploit errors in it.

Maintaining data security requires both a planned backup scheme and careful measures for access control.

For this reason, new updates should be installed promptly. The best way to do this is to use the automatic updates feature, but this requires reliable and fast Internet access. If your computer cannot access the Internet, the risk is less but you should still install updates whenever possible.

Firewalls

Any computer that connects directly to the Internet should have firewall protection. Attacks from the Internet are frequently automated, putting every unprotected computer at risk.

The simplest form of protection for a single computer is a software firewall. Some vendors offer anti-virus software and firewall software in the one package, which simplifies computer management.

If your network accesses the Internet via a router, the router should provide firewall protection, but be sure to ascertain that it does. If not, you should install a hardware firewall between the router and the network.

Internet Filtering

Internet filtering refers to the use of software to block access to undesirable Websites. Though a useful aid, filters should never be your only form of protection. There is no substitute for supervision.

Filters should be updated weekly because those who profit from the undesirable Websites are constantly changing their tactics to circumvent the software.

For stand-alone computers or those in a small network, filtering software

Picture Removed

can be installed on each computer. For larger networks, it is more efficient to install the software on a single computer that protects the whole network. Commercial products for protecting networks are quite expensive, but there are good free open-source alternatives.

Some Internet service providers include a filtering option with their monthly fee.

Usage Policies for Students and Staff

Most schools have an Acceptable Use Policy for onsite computers, and penalties for failure to comply with its provisions. It should include statements that address the following issues:.

1. Careful behavior around computers.

2. Restrictions on installing applications. Allowing unauthorized personnel to install applications opens the door for copyright infringement and increases the risk of introducing viruses.

3. A requirement that students obtain teacher permission before accessing the Internet. This also places an obligation on the teacher to provide appropriate supervision.

4. A requirement that students and staff observe copyright regulations relating to music, movies, and games as well as material for academic purposes. Schools risk heavy fines if they cannot demonstrate reasonable vigilance in preventing users from storing unauthorized copyrighted material on school computers. This applies to materials downloaded from the Internet or brought to school on CDs or other media.

5. What can and cannot be stored on school computers. Apart from copyright concerns, consider the problem of large files filling hard drives and students being distracted by material on the computers.

6. What constitutes appropriate material for students to access on the Internet, and a requirement that students discreetly notify the teacher if they inadvertently access inappropriate material is on the Internet.

7. Printing procedures and fees.

Any computer that connects directly to the Internet should have firewall protection.

Extra Support

If some of the advice and procedures described in this article sound like a foreign language to you, consider obtaining technical support. It would be prudent to explore support options before problems arise so that assistance can be obtained promptly when needed.

Some possible sources of help and answers to questions include the following:

1. Friends and parents in the school community. Free support can be valuable, but it may come with risks attached. Some people who offer free support may ignore copyright regulations. Others may have personal preferences that are incompatible with your school's needs or resources. Try to obtain advice from a range of sources.

2. Colleagues in larger schools.

3. Online communities. Many online communities have forums where you can ask questions and receive answers. A Google search can provide a list of such communities (i.e., http://teachers.net/mailrings/ or http://www.siec.k12.in.us/west/edu/list.htm. People in these forums are typically eager to answer questions, but some communities have a large volume of messages posted each day. You might prefer to join the new Adventist Virtual Leaning Network Community: http://www.avln.org/commuity, which also offers the opportunity to discuss other issues relevant to Adventist schools.

4. Paid support. Sometimes there is no alternative but to hire a computer technician to provide the support you need.

Budgets

Tight budgets often tempt schools to limit spending. However, items such as anti-virus software, access control, and backup schemes must be given a high priority because the costs of negligence can be devastating.

Items that should be purchased and upgraded as required include the following.

1. Backup devices such as DVD burners and portable hard drives.

2. Synchronization software or other backup software.

3. Anti-virus, anti-spyware, and firewall software.

4. Internet filtering software.

Items that require an annual budget allocation include the following:

1. Consumables such as CDs and DVDs, and small items such as Flash drives.

2. Updates and renewal of subscriptions for protective software (anti-virus software, etc.).

3. Upgrades for both operating systems and programs. How frequently you should upgrade depends on a number of factors, with security being a major consideration. Computers running MacOS prior to version 10 or Windows 95, 98, and ME pose a security risk.

4. Provision for paid support. While the cost of computer hardware has been decreasing steadily, security risks and the cost of protection have increased. Modern society's increasing dependence on technology makes it imperative that we do not ignore these risks.

For More Information

The Adventist Virtual Learning Network Community site http://www.avln.org/community offers both support and opportunities for collaboration. It provides detailed information on some of the issues mentioned in this article and links to other relevant sites. To obtain access, send an e-mail to community@avln.org.au. ✐

Peter Wallace *teaches Information Technology at Brisbane Adventist College in Queensland, Australia. He previously taught in small schools where looking after computers and their security was among his many responsibilities.*