Information Security Announcement Series for Principals

Purpose

In conjunction with Information Security Awareness Week in April, this series is a list of short tips for effective information security practices to be read during school announcements either during that week or the entire month. They can be read separately or in some sort of themed week format.

To be read each time

April <days> is Information Security Awareness Week, and in observance of this important subject, <school> will present an information security tip each day in order to make your home computer more secure. Today's important tip concerns <topic>:

Passwords

- Make passwords at least eight characters in length and use letters and numbers when creating them.
- Change your password regularly and make sure it's something you can remember without writing it down.
- Use a password that you can type quickly without looking at the keyboard, making it harder for someone to steal your password by watching over your shoulder.
- Don't use your login, your own name, your family's names or your pets' names in any form as your password. Never use publicly accessible information about yourself, such as social security number, license numbers, phone numbers, address, or birthdays.
- Don't use the "Remember Password" function. If someone were to steal your computer, it would become that much easier for him to get to all vital information on your system.

Viruses

A computer virus is a program written specifically to infect and/or alter other programs by self-replicating and attaching themselves to things like documents, presentations, and system files and can be spread by email, CDs, and floppy disks. There are four basic steps to computer virus protection. The first is prevention, which is the installation of virus protection software in order to detect, eradicate, and report viruses.

The second step of computer virus protection is detection, or making sure that once you buy anti-virus software, it is run on a regular basis so computer viruses can be found and destroyed.

The third step of computer virus protection is eradication. When a warning is given about a virus being detected on your computer, you must act quickly and quarantine the virus, delete it, and repair the compromised program.

The fourth and final step of computer virus detection is communication. If you still experience problems with your information system after running your anti-virus software, you might have a new virus that is unknown to those that create the detection software. It is your duty to inform the anti-virus software creators about activity that might be related to viruses so they can find ways to eradicate them.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Physical Risks

Hard drive crashes are a common cause of information loss; regular system backups are the only effective remedy for making sure your information is safe. Store important information on disks, so if the hard drive fails, you still have that information stored somewhere else.

Power problems also cause damage to a computer by harming the hard drive. Protect your computer from such threats by using surge protectors and uninterruptible power supplies.

Computer Ethics

Begin each day with: Just as much as there are rules for saying and doing certain things in the real world, there are rules for conducting yourself in the cyber world. The Computer Ethics Institute has defined The Ten Commandments for Computer Ethics, and today's is:

Thou shalt not use a computer to harm other people. This would include not just hacking into another computer, but also using websites or email to send out hateful information about someone else, a school, or place of business.

Thou shalt not interfere with other people's computer work. This would be any sort of interruption in someone's normal routine online or at his computer. Although you'd probably like to put pop-up ads in this category, you really can't.

Thou shalt not snoop around in other people's files. Any time you look at someone else's files without probable cause, you're in violation of their right to privacy.

Thou shalt not use a computer to steal. Never take anything off someone's computer without permission.

Thou shalt not use a computer to bear false witness. Don't use your information system in order to lie about other people or events.

Thou shalt not use or copy software for which you have not paid. You are permitted to make one copy of a program for personal use, as long as neither the original nor copy will be used at the same time.

Thou shalt not use other people's computer resources without authorization. Just as your child should ask first before they use someone else's things in the real world, they should ask before they use someone else's space on their computer, their web page, or email.

Thou shalt not appropriate other people's intellectual output. This will probably be the hardest one on the list to explain to your child. With file sharing programs so abundant and everyone taking advantage of them, it will be difficult to show your child that it's illegal and people suffer from the theft of their property, whether it's a TV or a song.

Thou shalt think about the social consequences of the program you write. Anything that anyone could potentially see needs to be looked at in terms of whether or not it could hurt others emotionally or threaten someone in some way. Laws in cyberspace apply just as much as they do in the real world, and harassment is harassment anywhere.

Thou shalt use a computer in ways that show consideration and respect. You should always use your information system in a way that is never harmful to anyone else, whether it's by word or deed.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu