The Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University presents:

Five Steps to Becoming an Information Security Expert!

Information Security Basics for Students

What is Information Security? And, why do kids need to know about it?

"Information Security" refers to protecting important files, documents, and programs that are stored on the different parts of a computer. This includes protecting your schoolwork, games, or important personal information that you, your parents, or your teachers may keep on the computer.

Kids need to know about Information Security, so that they can help to protect these important documents. By learning how to be "security experts", kids can teach others the basics of Information Security.

There are 5 Steps involved with becoming a security expert. Each of the steps is listed and described below. After practicing these steps, you'll always be in the habit of being secure!

Step One: Protect Your Password!

When you log in to use your computer at home or school, you may need to enter a password in order to enter the system. It is really important to protect that password by keeping it a secret from people who do not need to know it. More than likely, you will need to share your password with your parents and/or teacher…and that's OK. But, it is NOT a good idea to tell your friends, lab partner, or strangers about your password.

What's the big deal about a password? What can happen if someone finds out what mine is?

Well, there are a couple of reasons why it is really important to protect your password. First of all, someone could use your password to enter your email system. Once they have access to your email, they could send mean letters to all of your friends. The emails would look like they came from you, and your friends would probably be upset. Or, the person could use your email

account to send viruses or malicious code to all of your email pals. Once again, it would look like you were the one who did all of the damage. What a mess to get out of!

Another reason to protect your password is in order to protect your own personal work. For example, if someone got your password at school, they might be able to go into your files and change some of the words or pictures. The person making the changes might think this is funny, but if that file contained your big project or homework assignment…you may not think it was funny at all. In fact, you may not be able to recreate the project as it was before, and that could hurt your grade in class.

Finally, you want to protect your password so that you can protect important information that you might have stored on your computer. For example, maybe you have a hard time remembering the combination to your locker for gym class. So, you decide to type in the combination and store it in your network folder. If someone nasty gets a hold of your password, they could find the combination and damage or steal your property.

Now that you know why to protect your password…*how do you do it?*

Below you will find some guidelines to follow when using passwords:

1. Do NOT post your password or store it near your computer.
2. Do NOT write your password in an obvious place such as on your class folder, your hand, or your backpack.
3. Make sure that your password is at LEAST 8 characters long.
4. Be sure to use numbers, punctuation marks, and capital letters in your password:

   Good Examples: Boiler*Maker

   12girl#power

   Iam@work

   iLUV2B@chs

5. Do NOT use passwords that are easy to guess:

   Bad Examples: password (this is the most commonly used password!)

   123456

   computer

6. Try to pick passwords that are not too easy for others to figure out:

   Avoid Using: your name
   your best friend's name
   your address
   your birthday
   your school name

7. Do NOT share your password with your friends. A true friend would understand why you need to keep it private.
8. Try not to type your password when other people are watching.
9. If you think someone saw you type in your password, ask your parent/teacher to help you get a new one.
10. ALWAYS remember to log out of the computer that you are working at! This is really important if you are checking your email in a public place!

Step Two: Keep Your Files Safe!

Keeping the files and documents that you store on your computer safe is really important. Imagine if you had just finished writing the *best* book report ever---and then your electricity goes out and you lose your document. Or, what if the computer you are working on malfunctions and deletes all of your work on a big project that is due the next morning? Or, what if someone stole your computer that had ALL of your science fair project on it? What would you do? What if you didn't have time to do it over?

Sometimes, there is no way to prevent the loss of your work. But there are some steps that you can take to be sure to protect your work. First, we need to identify the different types of "threats" that occur with computers. There are 3 different types of threats to your files that you should be aware of:

1. Natural Threats: These threats cannot be controlled and occur directly through nature. Examples include: tornados, lightning, floods, snow-storms, and earthquakes.
2. Intentional Manmade Threats: These are threats caused by people who are trying to do harm. These people *intentionally* try to cause

damage to computers. Examples include: stealing computers, vandalism, purposely sending viruses, and hacking.

3. Unintentional Manmade Threats: These are threats caused by people who did not mean to cause any harm. These people have accidentally caused damage to computers. Examples include: spilled beverages, accidentally deleting files, equipment failure, power outages, and viruses.

So, now that we know about the three types of threats to our computers…*what can we do to help protect our important work?*

Here are some guidelines to follow to keep your files protected:

1. Make Back-ups!! It is really important that you get in the habit of making a back-up copy of any file that you want to protect. To do this, save your work on a separate disk that is NOT connected to your computer. Keep that disk in a safe place. By doing this, you have a made a SECURE copy of your work that you will have available to you even if the computer you work on blows up!

   Note: Your back-up copy needs to be saved in a different location than your original. Consider this: *What if you stored the original file and your back-up on the same disk and then you dropped that disk into the ocean? Would you have your back-up to use? What would have been a better thing to do?*

2. Do Not Have Drinks Near Your Computer! Even though you may work up quite a thirst while working on a school project, it is NOT a good idea to keep liquids near your workstation. We all know how easy it is to spill a drink…and liquids can cause a really big mess when they land on computer equipment, disks, or near electrical outlets. Not only could you lose your work, you could also cause harm to yourself! If you do get thirsty, take a break and enjoy your drink outside of your workstation area.

3. Print out and Keep a Paper Copy of Important Work: It is also a good idea to print out a copy of important work (reports, projects, etc.), just in case you can't recover your original electronic version. At least with the paper copy (also called a "hard copy"), you would have a record of the information you had written.

4. Clearly Label Your Disks: It is really important that you organize your files on your disks and that you keep your disks clearly labeled. For example, if you have a monthly book report to turn in for your social studies class, you may want to consider saving them all on the same disk which is labeled as "Social Studies—7th Grade". Most disks come with stickers that you can easily put on the outside of your disk. If you do not have labels, use a permanent marker.

   It is also a good idea to save your files with a name that you will understand. From the example above, that student may wish to save his documents by the last name of the author that he wrote his report about. (Ex: twain, rowling, cleary) By doing this, he can easily find the report if he needs to use it again.

5. Keep Magnets Away From Your Computer and Disks! Magnets will erase the information stored on disks and computers. It happens quickly, so be sure to keep your magnets far away from your workstation.

Step Three: Things to Remember While You are Working Online:

When you are using the Internet at school and at home, it is VERY important to remember that you need to use it responsibly. The computer equipment, Internet access, and everything else in your classroom belongs to your school. When you use these tools, you are reflecting upon the reputation of the school. Your actions will serve as a credit or discredit to your school.

By following the basic safety guidelines listed below, you will be helping to protect your school, your files, and yourself from harm.

1. NEVER give out your personal information without permission from your parent or teacher. "Personal information" includes: your name, address, phone number, parent information, school information, etc. If you are on a site that asks you for this information, immediately tell your parents and/or teacher!
2. Chat rooms, personal email, online games, etc. are OFF-LIMITS when you are at school. Many times, these types of environments can lead to trouble. If your parents allow you to use these at home, it is CRITICAL that you remember to NEVER give out personal information

about yourself, your parents, or your school. If anyone says anything nasty to you---or makes you feel uncomfortable, IMMEDIATELY go tell your parents. But, remember, these places are NOT for school use.

3. Tell your teacher IMMEDIATELY if you come across information, words, or images that make you feel uncomfortable, or that you know are inappropriate.
4. NEVER open files or email from people that you do not know. They may contain a virus.
5. NEVER give out your password. (This includes friends, lab partners, and especially anyone online!)
6. Do NOT send pictures/information to anyone that you do not know.
7. While using technology at school, it is very important to remember to stay focused on the assigned task. By not following the directions of your teacher, you may risk losing your chance to use the computer.

Step Four: Use Kid-Friendly Search Engines:

The most important idea to remember when you are looking for information on the Internet, is that ANYONE with a computer and an Internet connection can post a site on the Web. This is one of the reasons that the Internet is so great; everyone can have a chance to express their creativity. It is also why the Internet is NOT so great; it allows people to post sites that contain dishonest information, mean pictures, or nasty attitudes.

One easy way to prevent running into some of those "nasty" sites, is to use a Kid-Friendly Search Engine. A "search engine" is a program found on a Web site that searches the information on parts of the WWW for specific words that you have typed in. Once it finds all of the "matches" for your keywords, the search engine will list the sites it found.

Kid-friendly search engines work the same way. The best part about these particular search engines is that they will find great sites without including ones that contain violent images, swear words, or other inappropriate information. Using a kid-friendly search engine will save you time by sorting through the "junk" sites before you even have to see them. This will help you to find the information you need much more quickly!

Step Five: Making Sure That Web Sites are Worthwhile:

As a general rule, if you come across a site that makes you feel uncomfortable, or that you know is inappropriate for school…tell your teacher or parent immediately. If they are not around, close down your Internet connection and go find them. Remember to use "Kid-Friendly Search Engines" to help avoid sites that are not right for you!

So, how do you know which sites to trust? How can you tell if a site is worth using as a reference for your schoolwork? The best answer to these questions is to take a look at the background of the sites and ask a series of questions. Consider using the questions listed below:

1. What is the intent or purpose of the site? Look carefully at the content that is included on the site. Is something being sold? Is there a hidden purpose? Is the site trying change your opinion about something?

   If you answered "yes" to any of the above questions, the information contained on that site may be biased. It will be important for you to determine whether the information is fact or opinion based.

2. What is the Background of the Person/Organization Behind the Site? Does the person or organization that posted the site provide background information? Is there a way to contact the Webmaster for further information?

   If you answered "no" to those questions, it may mean that the person posting the site does not have a strong background in the content area. Or, it may also mean that they do not want to be known for posting the Web site. Either way, a site without a contact person/organization can mean trouble.

3. What is the Age of the Site? How old is the site? When was it last updated? Has it been abandoned?

   It is really important for you to know when the information on a Web site was written. If the site is old, abandoned, or undated, the information it contains may be outdated and no longer true. Sometimes, the information won't change (ex: the day Pearl Harbor was bombed), but some information changes rapidly (the name of the most popular movie at the box office). Ask your teacher or parent to

help you determine if the page is too "old" to contain relevant information.

4. What Type of Content is Included? Is the information on the site useful? Is the information on the site related to the purpose of the site? Is the site free from obvious typographical errors?

   If you answered "no" to the questions listed above, the site in question may not be the best resource for you. When you are looking for a site to use as a reference, it is important to find a site that contains credible (trustworthy) information. If a site is NOT well organized, contains many spelling errors, or refers to topics that are not related to the purpose of the site, it lowers the level of credibility of the site. The person or organization who posted this site may not really be a person who knows a lot about the topic; instead, the Webmaster may just be a person who knows a tiny bit about the topic---and is not an expert at all.

5. What is the Design of the Site Like? Is the site easy to use? Is the site set up to provide easy access to the information? Does the site offer a way to ask questions of the expert?

   If you answered "yes" to the questions above, chances are that the site is a good one. The people who have posted the site have taken the time to make sure that you could find information and ask questions if you need to.

When you are evaluating a Web site, it is really important to think about all five of the questions listed above. You will need to consider ALL of those areas before you decide whether or not a particular site is useful.

Well, that's it! Those are the 5 Steps involved with becoming a Security Expert! Remember to practice them everyday in order to protect your work, your school, your computer, and *most importantly* yourself from danger!

If you have questions, comments, or suggestions about the 5 Steps to becoming a Security Expert…

Visit CERIAS K-12 at: http://www.cerias.purdue.edu/K-12
Or, contact: Judy Lewandowski at judyL@cerias.purdue.edu