

The Educator's Role in Safe Computing

The Educator's Role in Safe Computing

Q-CERT K-12 EDUCATOR'S WORKSHOP 1

PREPARED BY: WIAM YOUNES

Introduction

Educators in K-12 schools play many roles in relation to their students — as teacher, authority figure, facilitator, mentor, counselor, and as protector.

Educators play these roles naturally and diligently both within and beyond their subject areas. Just as they assume these roles in the physical and social environment of their schools, educators must also play them in the realm of cyber security.

Educators do not usually receive adequate information about cyber security or training in how to teach the concepts and practice the principles of cyber safety, unlike well-established subject areas like math, science, and languages.

Safe computing education includes three main subjects:

1. cyber security
2. cyber ethics
3. cyber safety

This workshop gives an overview of cyber security for K-12 educators. To begin, let us first share a common definition of cyber security:

Cyber security is a set of principles and practices designed to teach you how to safeguard your computing assets and online information against threats.

Technology in Schools

The use of technology is ubiquitous; daily life both in schools and out is heavily reliant on a large variety of tech tools. The majority of the technology we use for communication is connected to the internet – the worldwide network of networks that defines our concept of virtual or “cyber” space.

The internet is a global network that connects over one billion people and more than 600 million computers. More than 100 countries are linked into exchanges of data, news, and opinions. ¹

No doubt, you are familiar with many of the technologies connected to the internet that educators use in and out of schools:

- computers, for
 - ◆ web browsing
 - ◆ email
 - ◆ chat rooms
 - ◆ instant messaging
 - ◆ web-based educational software
 - ◆ media
- personal digital assistants (PDA), for
 - ◆ data communication
 - ◆ voice communication
 - ◆ media communication
 - ◆ global positioning
- cellular phones
 - ◆ data communication
 - ◆ voice communication
 - ◆ media communication
 - ◆ global positioning
- digital cable or satellite television
- ATM machines, credit cards, and debit cards
- global positioning system (GPS)

“But it’s not my job - computer safety is the responsibility of the school’s technology personnel!”

Many educators hide behind this excuse to relieve themselves from the responsibility of teaching and practicing safe computing in their classrooms. However, as much as we might wish, cyber security is *not* limited to technology teachers and administrators. In today’s world, *all* school personnel must be aware of cyber security practice and adhere to its principles in order to create a safe environment for students, educators, and staff, and to protect the school’s assets. Similarly, teachers in subject areas different from technology can incorporate aspects of cyber security into their lesson plans.

¹ www.internet.com

As an educator, it is essential to understand the nature and cause of cyber threats, their potential effects, and the solutions available to protect yourself, your students, and your school. As an educator, once you have a command of cyber security knowledge, it is natural for you to want to teach it to your students, colleagues, and their families.

Cyber Threats

There are a few main categories of cyber threats to learn and to educate your students about. They include

- a. piracy – illegal use of copyrighted material such as plagiarism or illegal downloading of music, movies, text, or other types of files
- b. intrusion – unauthorized individuals trying to gain access to computer systems in order to steal information, corrupt files, illegitimately view data, or gain control of the computer. In schools, as in any organization, intruders can be outsiders or insiders.
- c. identity theft – computer intruders intent on stealing your personal information to commit fraud or theft
- d. predatory behavior – online behavior that targets some aspect of your online information in order to steal or destroy it
- e. viruses – a self-replicating program that spreads by inserting copies of itself into other computer code or into documents
- f. spam – often automated programs designed to send a message to multiple users, mailing lists, or email groups
- g. worms – a self-replicating, self-spreading malicious computer program
- h. Trojan horses – a malicious program disguised as legitimate software
- i. malware – programs that are designed to harm your computer
- j. spyware – software that sends information from your computer to a third party without your consent

Effects of Cyber Threats

Cyber threats can affect you, your family, students, colleagues, and school in many different ways. The disruption from threats can vary from the corruption of one or two files or a simple virus to mass corruption of the entire school network that destroys important data stored on the network.

Here are some examples of how you could become a victim (or unwitting cause) of a cyber threat and potential consequences:

- a) If you or a student deliberately or unknowingly download or redistribute copyrighted material (or a computer under your supervision is used to do so), this illegal use could result in legal fines, job loss, or action against you from law enforcement officers (depending on the severity of the action). For instance, students in American universities who illegally download or distribute copyrighted files are often caught and fined or expelled, and if they are high school students or younger, and are caught using a parent's computer or internet connection, the parent can also suffer legal consequences.
- b) An intrusion into a school network by an individual in the school (i.e., an "insider" such as a colleague or student) or by an individual not at the school

(i.e., an “outsider”) could have bad results: data alteration, such as the changing of grades; theft or destruction of test materials; stolen information that could be used for identity theft of anyone in the network; or copying and destroying other data belonging to you or to the school.

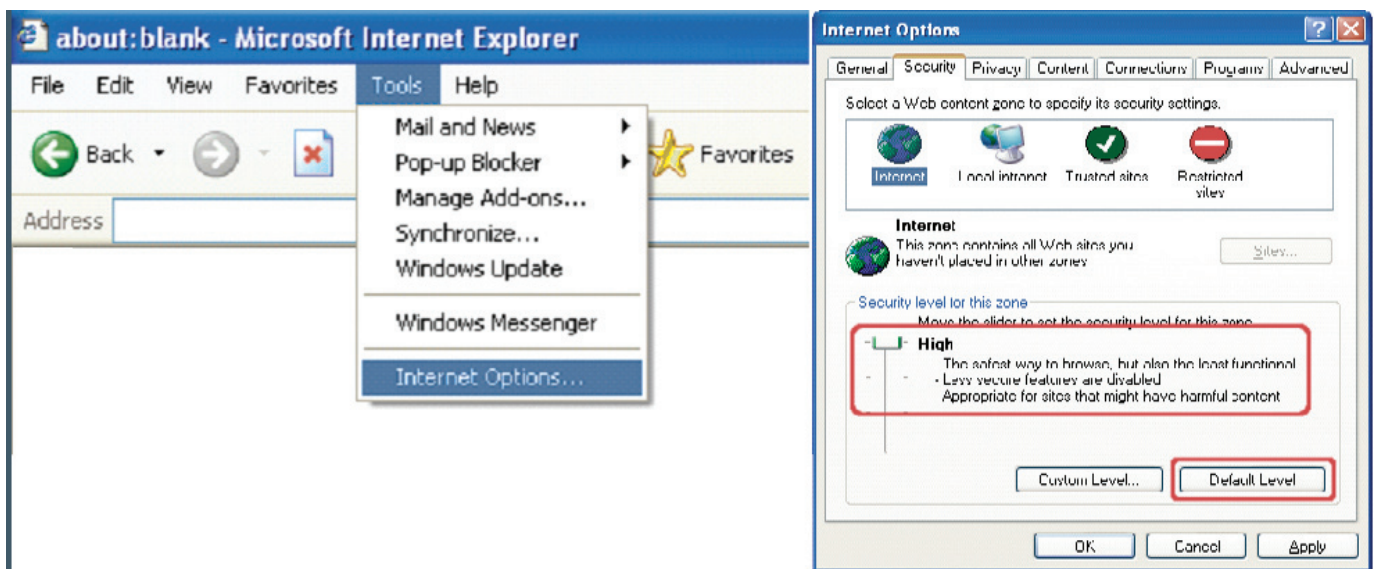
- c) By clicking on advertising pop-ups or on attachments sent to you via email, instant messaging (IM), or in a chat session, you could receive hundreds of unwanted email (spam). Some attachments or software hidden in attachments could also access your email address lists and forward more unwanted messages or code to everyone on your list and then on to your contact’s lists and so on. Pop-up advertisements and attachments could also sometimes hide spyware which can enable a remote intruder to view everything on your computer as long as you are connected to the internet.
- d) If you receive and accidentally redistribute a virus, malware, worm, or Trojan horse from an email attachment, infected file, or document, any one of these can infect more documents, alter or destroy software, or disrupt the whole operating system on your computer. These malicious types of code can cause documents to be deleted, data to be stolen, and access to your computer to be interrupted. Malicious code can infect a school’s entire network as well as the computers and networks of other contacts.

How do you protect against cyber threats?

So how do you protect your data, your computer, and the school’s data and network? We recommend the following basic set of practices to protect against cyber threats:

1. Create a “strong” password. Strong passwords or passphrases consist of at least eight characters and include a mix letters, numbers, and symbols.
Your password is your unique key to the information you have, so don’t share it with your colleagues and family members. Be certain to uncheck the box that prompts you for your computer to remember your password.
2. Lock your computer at school or at home when you step out of the room or when you are not using the computer – unlocked computers are an open invitation for intruders (or even curious children!) to access your information or accounts. Most operating systems allow you to set a password that will prompt you if you want to access the computer once the screensaver has started.
3. Create unique user IDs for anyone using your computer. If you share your computer with students or others, as is the case in many classrooms, log off when you are done using it and provide other users access through a generic ID.
The ID can be set by your technical support personnel (such as “student user”) and can be created to limit user actions and privileges. Rarely should you allow anyone else “administrative” privileges on your computer.
4. Always assume your email, chat sessions, and text messages are not private. Anything you send over a network, unless it is strongly encrypted, could be read, changed, or forwarded anywhere, at anytime. Most of the internet is a public forum where anything you post online could potentially be viewed by millions and will not be erased, ever.
5. Use caution when opening an unexpected email. Email from people you don’t know, or unexpected email from someone you do know, are likely the result of a spam or are infected with a virus. Delete these types of email without opening them. If you think a friend is emailing you unexpectedly, call them to ask, and then run a virus check on the attachment before opening. Note you can configure some antivirus software to inspect incoming email automatically.

6. Back-up your data. Back up all important files, information, programs, and folders every time a change is made (or at least once a week). Keep your backups in a safe place.
7. Be wary of file sharing or sharing your computer with others. File sharing is the practice of making files available for other users to download over the internet from one computer to another (sometimes called a “peer to peer [P2P] model”). File sharing allows you to download files and exchange data. Sharing a computer also introduces the same risks as remote file sharing – someone may infect your computer on purpose or accidentally.
8. Update your anti-virus program and virus definitions as well as your anti- spyware software. Anti-virus and anti-spyware software scans data and software files on your computer for certain patterns that may indicate an infection. It is important to update this software frequently to have the latest virus definitions or spyware profiles available. Many of these programs allow you to set them to automatically update themselves and scan your computer regularly.
9. Use and maintain a firewall. A firewall acts like a guard, keeping potentially dangerous files, requests, or programs from accessing your computer. You can also set up your firewall to block access to certain web sites and allow access to others.
10. Set your web browser security option to a high level of safety. You can set your browser security on high to block access to undesired web sites. (Note that choosing a high safety setting may reduce some web site functionality if the site uses Java, Flash, or other enhanced web features.) To choose high safety in the Internet Explorer web browser, you would go to “Tools” on the menu bar, then click on “Internet Options.” This calls up a menu which enables you to set your security to low, medium, or high (see the screenshot below for an illustration).²



² Please refer to the document “Securing your Web Browser” on the US-CERT.gov web site for more detailed instruction: http://www.us-cert.gov/reading_room/securing_browser/

11. Enable your “pop-up” blocker. For the Internet Explorer web browser, on the tool bar, select “Tools,” then on the drop down menu select “Pop-up Blocker.” Click it and enable the tool to stop unwanted pop-ups from appearing during web browsing.
12. Disconnect your computer from the internet when not in use. Some types of malware are programmed to destroy your computer once you are logged off, but are still connected to the internet; others trigger malicious actions when the computer is in screen saver mode.
13. Take care when opening an attachment you receive through email, chat rooms, or SMS. Attachments can contain viruses, worms, or spyware, so scan your attachments before opening them. Do not open an attachment sent by someone you don’t know or that has a name or subject title that does not make sense to you.
14. Update your computer with the latest security patches for the software and operating system you use. Software and hardware companies frequently issue updates, called “patches,” to correct vulnerabilities. These patches fix the problem found in their operating system, browser, or software. Some companies issue regular security patches; for instance, Microsoft releases updates once a month. You can configure many operating systems to automatically download and install security patches. Check the web site of the company that makes your computer operating system or web browser, such as Microsoft or Apple. You can also visit the Q-CERT web sites to find information about computer security patches and vulnerabilities.

Teaching Cyber Security

Now that you have information about cyber security, how can you teach it to students in your class? (For this exercise, imagine you teach Arabic literature.)

Here is one example: You are teaching poetry and your lesson today is about Imru’ al-Qais. As an activity, you request that students research the era he lived in and the story behind one of the most famous Al Muallaqat poems in the history of Arabic poetry. You ask them to use the school’s computer lab to research the topic or give it to them as homework due in their next class. In your activity document and guidelines, make sure to provide your students at least one paragraph describing copyright guidelines, along with two to three tips on how to distinguish whether a web site is a credible reference or not.

References

www.qcert.org
www.us-cert.gov
www.mysecurecyberspace.com
www.webopedia.com
www.internet.com
www.csialliance.org



For more information about Q-CERT, contact info@qcert.org



