

Program Name
Staff Responsible for Lesson

MVCTC EL/Civics Program
Mary Ann Oatney

Date(s) Used	11/18/2009																				
Civics Category	II. Civics Participation																				
Civics Objective	16: Community Resources – Security: Describe ways to prevent and avoid becoming a crime victim. Describe ways, such as neighborhood watch, to prevent personal accidents a avoid becoming a crime victim.																				
Time Frame to Complete Lesson	1 - 2.5 hour session																				
EFL(s)	NRS Levels: 3-5																				
Standard(s)/Components of Performance	<ul style="list-style-type: none"> √ Listen Actively √ Speak so That Others Can Understand √ Read With Understanding √ Convey Ideas in Writing 																				
Benchmark(s)	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid black;">Listening</th> <th style="text-align: left; border-bottom: 1px solid black;">Speaking</th> <th style="text-align: left; border-bottom: 1px solid black;">Reading</th> <th style="text-align: left; border-bottom: 1px solid black;">Writing</th> </tr> </thead> <tbody> <tr> <td>L3.1 L4.1 L5.1</td> <td>S3.1 S4.1 S5.1</td> <td>R3.2 R4.1 R5.1</td> <td>W3.6 W4.6 W5.6</td> </tr> <tr> <td>L3.4 L4.4 L5.3</td> <td>S3.3 S4.3 S5.3</td> <td>R3.4 R4.4 R5.4</td> <td></td> </tr> <tr> <td></td> <td>S3.4 S4.4 S5.4</td> <td>R3.5 R4.5 R5.5</td> <td></td> </tr> <tr> <td></td> <td></td> <td>R3.6 R4.6 R5.6.</td> <td></td> </tr> </tbody> </table>	Listening	Speaking	Reading	Writing	L3.1 L4.1 L5.1	S3.1 S4.1 S5.1	R3.2 R4.1 R5.1	W3.6 W4.6 W5.6	L3.4 L4.4 L5.3	S3.3 S4.3 S5.3	R3.4 R4.4 R5.4			S3.4 S4.4 S5.4	R3.5 R4.5 R5.5				R3.6 R4.6 R5.6.	
Listening	Speaking	Reading	Writing																		
L3.1 L4.1 L5.1	S3.1 S4.1 S5.1	R3.2 R4.1 R5.1	W3.6 W4.6 W5.6																		
L3.4 L4.4 L5.3	S3.3 S4.3 S5.3	R3.4 R4.4 R5.4																			
	S3.4 S4.4 S5.4	R3.5 R4.5 R5.5																			
		R3.6 R4.6 R5.6.																			
Materials	Handouts: Internet Terms Internet Dangers How to Stay Safe on the Internet Test and Answer Key																				
Activities	<p>I. Internet Vocabulary - <u>Handout</u>: Internet Terms Review terms on the handout. Have Ss read and pronounce each term.</p> <p>II. Dangers on the Internet - <u>Handout</u>: Internet Dangers Discuss the dangers as listed on handout. Ask Ss if they have encountered any of these dangers; what did they do.</p> <p>III. How to stay safe on the Internet: <u>Handout</u>: How to Stay Safe on the Internet Read and discuss safety measures as listed on handout.</p> <p>IV. Written test: <u>Handout</u>: Fill In the Blanks</p>																				
Assessment/ Evidence	Students will pass the written test with 85% accuracy.																				
Reflection	Due to the technical content of this lesson, upper level ESOL students were targeted for this lesson plan. Most students were acquainted with some of the Internet terms and had practical experience using the Internet. Presentation and discussion of the dangers of the Internet were of great interest to them and several shared experiences they had. Their new awareness of the dangers gave them insight as to avoiding certain websites and interaction with others online.																				

EL/Civics Lesson Plan: Internet Safety

Length of lesson: With students who are familiar with using the Internet this lesson could be completed in 2-3 hours.
Allow time for questions.

I. Internet Vocabulary - Handout: Internet Terms

Review terms on the handout.

Have Ss read and pronounce each term.

II. Dangers on the Internet - Handout: Internet Dangers

Discuss the dangers as listed on handout.

Ask Ss if they have encountered any of these dangers; what did they do.

III. How to stay safe on the Internet: Handout: How to Stay Safe on the Internet

Read and discuss safety measures as listed on handout.

IV. Written quiz: Handout: Fill In the Blanks

Internet Terms



Internet: A network of millions of computers from all over the world.

email: allows people to send messages with pictures and sounds from their computer to any other computer in the world.

profile: short resume that lets other web users know something about you.

Java: programming language

search engine: program that searches information on the worldwide web by looking for keywords and returns information on that topic.

chat: typing and sending messages that appear almost instantly on the computer monitors of the other people who are participating in the chat.

chat room: place or location online where the chat is taking place.

bulletin board: An electronic message center

Facebook is a social networking website open to anyone 13 years of age or older. Users can create their own profiles with photos, videos, and information about themselves. Friends can browse the profiles of other friends and write messages on their pages. Facebook allows each user to set privacy settings. For example, if you have not added a certain person as a friend, that person will not be able to view your profile.

password is a secret word used to identify you when you log onto a Web site, i.e. email.

virus is a program that makes your computer crash or destroys files. Viruses are spread by email and file-sharing.

hacker is a person who accesses and changes information on other people's computers.

profile is a short story that lets other Web users know about you and your interests.

Twitter is a way of sharing information in the Internet with 140 characters or less.

blog are entries posted on a Web page.

Hit is a request made to a Web server.

MySpace allows friends to keep in touch you and for you to meet new people. Anyone using MySpace must be at least 14 years old. Once you sign up, you can write your information about yourself and upload photos of yourself and your friends. Once you have a profile on MySpace you can search or browse other users' profiles.

spam is junk email or postings.

filters are programs that screen Web pages to allow only certain information/pictures on the Web page.

flaming is posting or sending offensive messages over the Internet.



Internet Dangers

Internet can be a great tool for communicating with people, meeting new people, buying things, and downloading information, music, and movies. However many dangers can be found on the Internet waiting your users to download a virus or fill out a profile which uses personal information that may be used against you.

What are some Internet dangers?

1. **Internet scams** which offer good deals on buying product but the product is never delivered.

General Scam Indicators:

The scams described above are some of the most common types of Internet fraud. However, these fraudsters are clever people who may use many variations of the above scams to achieve their nefarious ends.

In general, be wary of unsolicited emails that:

- Promise you money, jobs or prizes
- Ask for donations
- Propose lucrative business deals
- Ask you to provide sensitive personal information
- Ask you to follow a link to a website and log on to an account.

Examples:

- ✓ A **phishing** scam is one in which victims are tricked into providing personal information such as account numbers and passwords to what they believe to be a legitimate company or organization. In order to carry out this trick, the scammers often create a "look-a-like" website that is designed to resemble the target company's official website. Typically, emails are used as "bait" in order to get the potential victim to visit the bogus website. Be wary of any email that asks you to click on a link and provide sensitive personal information such as banking details.
- ✓ **Nigerian Scams:** You may receive an email/letter/fax that asks for your help to access a large sum of money in a foreign bank account. The message says that you will get a percentage of the funds in exchange for your help.
- ✓ **Lottery Scams:** You may receive an email/letter/fax that claims that you have won a great deal of money in an international lottery even though you have never bought a ticket. The email may claim that your email address was randomly chosen out of a large pool of addresses as a "winning entry". Such emails are almost certainly fraudulent.
In all probability, the message is an example of the type of scam known as a Nigerian or "419" scam. The "large sum of money" does not exist.

2. **Viruses:**

- ✓ A computer virus is probably the best known and most dangerous threat to computer security. The most common symptoms that indicate your computer has been infected:

- files and data is deleted
- the computer takes longer to load programs/applications
- items and images on your screen are distorted and unusual images and text appears
- unusual noises come from your keyboard, hard disk
- hard disk operates excessively or is inaccessible
- disk space and filenames change for no reason

- ✓ computer viruses are contracted today through e-mail and by downloading software.

3. **Internet Auction Fraud:** Internet auction fraud is the most reported offense.

- The seller posts the auction as if he lives in the United States, but really lives in another country.
- The seller posts the auction under one name, and ask for the funds to be transferred to another individual.
- The seller requests funds to be wired directly to him/her via Western Union, MoneyGram, or bank-to-bank wire transfer. By using these services, the money is virtually unrecoverable with no recourse for the victim
- Sellers acting as authorized dealers or factory representatives in countries where there would be no such dealers should be avoided.
- Buyers ask for the purchase to be shipped using a certain method to avoid customs or taxes inside another country.

4. **Cyber-Stalking** (harassment)

- If someone on the Internet sends you a lot of e-mails, follows you into chat rooms, and/or sends you messages after you have stopped responding, that person may be harassing you.
- **False accusations.** Many cyberstalkers try to damage the reputation of their victim and turn other people against them. They post false information about them on websites. They may set up their own websites, blogs or user pages for this purpose. They post allegations about the victim to newsgroups, chat rooms or other sites that allow public contributions, such as Wikipedia or Amazon.com.^[4]
- **Attempts to gather information about the victim.** Cyberstalkers may approach their victim's friends, family and work colleagues to obtain personal information. They may advertise for information on the Internet, or hire a private detective. They often will monitor the victim's online activities and attempt to trace their IP address in an effort to gather more information about their victims.^[5]
- **Encouraging others to harass the victim.** Many cyberstalkers try to involve third parties in the harassment. They may claim the victim has harmed the stalker or his/her family in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit.
- **False victimization.** The cyberstalker will claim that the victim is harassing him/her. Bocij writes that this phenomenon has been noted in a number of well-known cases.
- **Attacks on data and equipment.** They may try to damage the victim's computer by sending viruses.
- **Ordering goods and services.** They order items or subscribe to magazines in the victim's name. These often involve subscriptions to pornography or ordering sex toys then having them delivered to the victim's workplace.
- **Arranging to meet.** Young people face a particularly high risk of having cyberstalkers try to set up meetings between

them.^[6]

5. Internet Identity Theft

- Identity theft is when your personal information is stolen and used illegally to open accounts in your name.
- Internet identity theft occurs Internet user is asked personal information, i.e. identification.
- Name, social security number and address is all that is needed to assume someone's financial identity.
- If you go through a link and give personal information, your account information can be taken.
- Once your personal information is taken, thief can open new accounts with your personal information and change your mailing address online. It may be months before you know something is wrong when you get your credit card bill with charges.

6. Credit Card Fraud

- Credit card fraud is theft or fraud committed using a fraudulent credit card to purchase things online.
- Purpose may be to get items or money from an account.
- If Internet site is not a secure site, your credit card information could be accessed by anyone associated with website and accessing the website.



How To Stay on the Internet

Do not post information that will identify you, including:

- Your full name
- Your home address or phone number
- Your social security number
- Passwords
- Credit card or bank account numbers
- Names of family members or friends
- Your workplace
- Your account password

Do not open links or files from people you do not know. 70% of internet crimes are through email scams.

Check Web site address for domain:

.com (commercial), .gov (government), .org (organization), .net (network), .edu (educational organization)

Never agree to send or accept money, gifts, or anything from someone you meet online.

Check out website's safety tips section. Look for the yellow lock in the bottom right corner of the screen. It means that your personal information is secure.

If you begin downloading something that you don't want, push "Stop" button at the top of your screen. This will stop the process.

Make sure you have updates virus protection software on your computer.

Do not download images, movies, or music unless you know the site is safe. Look for the yellow lock on the screen.

Test

Name _____

Date _____



Use the words from the list below to fill in the blanks.

- | | | | | |
|-----------------|-----------------------|-----------------|--------------|----------------|
| Internet | chat room | password | virus | profile |
| spam | bulletin board | hacker | blog | flaming |

1. _____ short resume that lets other Web users know something about you
2. _____ network of many computers from all over the world
3. _____ secret word used to identify you when you log onto a Web site
4. _____ junk email
5. _____ person who accesses and changes information on other people's computers without permission
6. _____ electronic message center
7. _____ entries posted on a Web page
8. _____ posting or sending offensive messages over the Internet
9. _____ sending message to other people who also chatting
10. _____ program that makes your computer crash and are spread by email and file-sharing

Test Answer key

Name _____

Date _____



Use the words from the list below to fill in the blanks.

Internet **chat room** **password** **virus** **profile**
spam **bulletin board** **hacker** **blog** **flaming**

1. **profile** short resume that lets other Web users know something about you
2. **Internet** network of many computers from all over the world
3. **Password** secret word used to identify you when you log onto a Web site
4. **spam** junk email
5. **hacker** person who accesses and changes information on other people's computers without permission
6. **bulletin board** electronic message center
7. **blog** entries posted on a Web page
8. **flaming** posting or sending offensive messages over the Internet
9. **chat room** sending message to other people who also chatting
10. **virus** program that makes your computer crash and are spread by email and file-sharing