### Program Name <u>MMVCTC EL/Civics Program</u>

Staff Responsible for Lesson Mary Ann Oatney

Date(s) Used	11/2007			
Civics Category	II. Civic Participation			
Civics Objective	II. 3—Community Resources—Advocacy Identify a local community need or civic-oriented complaint; research and address the issue.			
Time Frame to Complete Lesson	2 hours			
EFL(s)	High Beginner ESOL, Low Intermediate ESOL, and High Intermediate ESOL			
Standard(s)/Components of Performance	√ Listen Actively √ Speak so that others can understand √ Read with understanding √Convey ideas in writing			
Benchmark(s)		Speaking S3.1 S4.1 S5.1 S3.2 S4.3 S5 3 S3.3 S4.4 S5.4 S3.4 S4.5 S3.5	Reading R3.1 R4.1 R5.3 R3.2 R.4.4 R5.4 R3.4 R4.5 R5.6 R4.5 R4.6 R3.6	W2.3 W4.4 W5.3
Materials	Video: Culture Clips #5, Consumer Scams  VCR  Handouts: Culture Clips: Consumer Scams  Handout 1, Vocabulary  Handout 1A, Vocabulary  Handout 3, Partner Workout  Handout 5, Individual Activity  *Available from NEABLE—www.NEABLE.org  Handouts: The Bank Examiner  Top 10 List of Consumer Scams – 2008  Tips on How to Identify a Scam or Fraud  What can you do to defend yourself from scams, frauds  and identity theft?			

#### Activities

Using *Handout 3, Partner Workout for "Consumer Scams"*, have students break into pairs and ask each other the five questions on the handout. Regroup and share answers.

#### A. Show video, Culture Clips #5, Consumer Scams.

- Students will determine the two scams in the video and discuss the characteristics of each scam. Have students complete handout:: Culture Clips: Consumer Scams and review answers.
- Using Handout 1, Vocabulary for Consumer Scams and Handout 1A, Vocabulary, have the students work in pairs to complete. Reviews handouts as a class to check for understanding.
- Further discussion could center on personal experiences of the students with scams

#### B. What is a scam:

- Scam is a dishonest plan, usually to get money without receiving anything in return.
- Scammers look for an easy way to get something of value in the easiest way.
- Every scam starts like this:
  - o Scammer gathers some public information on a person
  - O Gets your name and address from a telephone book
  - Checks county records to see who owns houses where the person lives.
  - o Tries to trick a person into buying some unnecessary product.
- Before distributing the handout, The Bank Examiner, read the scenario and have the students identify the scam. Following discussion pass out the handout, read and discuss the information.

#### C. Avenues for scams. Discuss each.

- Telephone: someone calls, wanting you to donate money to a charity that doesn't exist or wants you to buy a product which you'll never get.
- Internet: online shopping, investments, bogus Web sites, email businesses
- Mail: prize awards, charity letters
- Classified ads: job ads, chain letters
- Door-to-door sales: selling products which don'
- Use handout:: Top 10 List of Current Scams 2008

#### D. Ways to Identify a scam. Ask:

- What is the first thing they say about themselves?
- Do they talk about the product or the service they offer?
- If the first thing you read is all about the money to be made, be careful.
- Do they have a real product?
- If there is nor real product and if it is just paying money, it is illegal.
- Review the tips on <u>handout</u>:: Top Tips to Protect Yourself Against Frauds and Scams, Identity Theft and Reduce Spam

	Email.
	<ul> <li>Student Activity: Have students break into groups. Assign each group a scam. Students are to identify the characteristics of the scam. Regroup and have each group present their scams to the class.</li> <li>E. Tips on Identifying a Scam: use handout, <i>Tips on How to Identify a Scam</i> <ul> <li>Read and discuss the elements of a scam on handout.</li> <li>Write unfamiliar vocabulary on the board.</li> <li>Discuss: Have any of the students been scammed? If so have them share their experiences.</li> </ul> </li> </ul>
	F. Using handout: What can you do to defend yourself from scams, frauds and identity theft?  • Review the list of what you can do to protect yourself.  • Remind students that they can sign up for the Do Not Call List:  1. WWW.DONOTCALL.GOV 2. 1-888-382-1222  • Obtain free credit report at:
	<ol> <li>annualcreditreport.com</li> <li>ftc.gov/bcp/conline/edcams/freereports/index.html</li> </ol>
	G. Students complete Culture Clips handout #5, Consumer Scams. Collect and review. Return to students and discuss.
Assessment/ Evidence	Student oral responses Student written responses on Culture Clips handout #5.
Reflection	Students had no encounters with scammers. But their gullibility indicated to me that they were prime targets. They seemed interested in class content and asked many questions.  Since our program has many refugees from third world countries, this topic seemed a must for discussion.



# Bank Examiner - a scammer

A phony bank examiner calls you and asks for your help in catching a dishonest bank employee. He asks you for your account in order to check and see if a dishonest bank employee is using your account number for fraud.

**NOTE:** Banks <u>never</u> use this procedure. Only scammers do.

If you are contacted by someone using this scheme, do not give your account number. Instead try to get a

# name and number from the person and immediately call the police.

### Tips involving phone call scams:

- If callers will not identify themselves, hang up.
- Never give out personal information on the phone.
- Single woman should use initials instead of firs names in the telephone book listings.

# Tips on How to Identify a Scam or Fraud

If the e-mail, phone call, prize or lottery notification has any of the following elements, we strongly suggest it is probably a fraud and you do not respond to it. Below are some general tips to recognize scams. Detailed information can be found from the menu buttons at left:

The name of the company is listed on this website somewhere as a scam.

The email matches one of the definitions or formats on this website.

The organization has no website and can not be located in **Google**.

The email or requestor asks for bank account information, credit card numbers, driver's license numbers, passport numbers, your mother's maiden name or other personal information.

The email or caller advises that you have won a prize - but you did not enter any competition run by the prize promoters.

The email claims you won a lottery (we know of NO legal lottery that notifies winners by email)

The mail may be personally addressed to you but it has been posted using bulk mail - thousands of others around the world may have received the exact same notification. Especially true if you find an exact or similar email posted on this website.

The return address is a yahoo, hotmail, excite.com or other free email accounts. Legitimate companies can afford the roughly \$100 per year that it costs to acquire and maintain a domain and related company email account.

The literature contains a lot of hype and exaggerations, but few specific details about costs, your obligations, how it works, etc.

The prize promoters ask for a fee (for administration, "processing", taxes, etc.) to be paid in advance. A legitimate lottery simply deducts that from the winnings! The scheme offers bait prizes that, if they are real, are often substandard, over-priced, or falsely represented. Or, as part of the prize you can purchase "exclusive items" which may also be over-priced or substandard.

To get your prize might require travel overseas at your own cost (and personal risk) to receive it.

# **Top 10 List of Current Scams - 2008**

For detailed explanations of each scam, how to report a scammer and how to protect yourself, click on the blue titles below for more information! For internet crime and fraud statistics, see this page.

1. <u>LOTTERY SCAMS</u> These include scams which can go under the name of genuine lotteries like the UK National Lottery and the El Gordo Spanish lottery. Unsolicited email or telephone calls tell people they are being entered or have already been entered into a prize draw.

Later, they receive a call congratulating them on winning a substantial prize in a national lottery. But before they can claim their prize, they are told they must send money to pay for administration fees and taxes. The prize, of course, does not exist. No genuine lottery asks for money to pay fees or notifies it's winners via email.

- 2. <u>INTERNET AUCTION FRAUDS</u> Auction frauds (commonly called Ebay or PayPal scams, after the two largest venues) is a misrepresentation of a product advertised for sale through an Internet auction site or the failure to deliver products purchased through an Internet auction site.
- 3. <u>NIGERIAN ADVANCE FEE FRAUDS</u> These frauds take the form of an offer, via letter, e-mail or fax, to share a huge sum of money in return for using the recipient's bank account to transfer of the money out of the country. The perpetrators will often then use the bank account details to empty their victim's bank account. Often, they convince the victim that money is needed up front, to pay fees or is needed to bribe officials.
- 4. PHISHING AND PHARMING FOR IDENTITY THEFT The victim receives an email that appears to be from a credible, real bank or credit card company, with links to a website and a request to update account information. But the website and email are fakes, made to look like the

real website.

5. Get rich scheme and scam websites - Make \$\$\$ in your spare time! It so EASY once you get their free book or cd and learn their secrets! Sure... These websites are themselves scams; claiming to offer you a good deal, when at best, their products are worthless, they have no real secrets, and worse, some are identity thieves!

### 6. LOTTERIES AND OTHERS THAT SEND YOU A COUNTERFEIT

**CHECK** You receive a check in the mail - either from a lottery you "won" (without buying a ticker) or from an EBay buyer or other source. It looks real... but after you try to cash it, you find out it is a fake; and you're arrested for passing a counterfeit check!

### 7. FREE CREDIT REPORT.COM

The name of the website is freecreditreport.com, but you'll only get a credit report when you sign up for their paid service. And worst of all there IS a government mandated website where you CAN get a free credit report!

8. WORK-AT-HOME SCAMS Work-at-home and business opportunity scams are often advertised as paid work from home. After the would-be worker applies, they are asked for money up-front to pay for materials and, after paying, they hear nothing back.

A variation of this is, people are asked to invest in a business that has little chance of success.

**9.** PROPERTY INVESTMENT SCHEMES Investors attend a free presentation, which aims to persuade them to hand over large amounts of money to enroll on a course promising to make them a successful property dealer, usually involving "no money down". Schemes can involve the offer of buying yet-to-be built properties at a discount. Other variations include a buy-to-lease scheme where companies offer to source, renovate and manage properties, claiming good returns from rental income. The properties are generally near-derelict and the tenants non-existent.

10.900 PHONE NUMBER SCAMS Postal notification of a win in a sweepstakes or a holiday offer in this scam includes instructions to ring a premium rate number. This is generally a 900 toll number. Calls to the number incur significant charges, the recorded message is lengthy, and the prize often does not exist. It is a scam that has been around a long time, but it is still in use.

# What can you do to defend yourself from scams, frauds and identity theft?

Whether you think you have been the victim of a fraud or scam or want to be proactive in protecting yourself, here is a list of specific and simple actions that you can take, some just once, to protect yourself and your family! We have ranked them in order that you should take them:

- 1. **Don't use or carry a checkbook**. Pay by cash or credit card. Paying your bills through your bank or credit union's online bill paying service (which is usually free) is much safer than mailing a check.
- 2. Buy and use a paper shredder. Shred any documents that have your social security number or other financial information, such as your bank account numbers, credit card numbers etc. Identity thieves actually go through homeowner's trash to obtain personal information.
- 3. Sign up on the **Do-Not-Call List**
- 4. Sign up to block credit card offers from arriving in your mailbox.
- 5. Don't carry your Social Security card with you. When you renew your driver's license, make sure the DMV does not use your Social Security number as your driver's license number.
- 6. Use a separate email address when you post messages to any public forum, such as newsgroups and mailing lists. Free email accounts from <a href="Yahoo">Yahoo</a> and <a href="Hotmail">Hotmail</a> are perfect for this. Never use your personal email address for this purpose: you will be flooded with spam. You can periodically check this

- email account to see what's spam and what isn't. A bonus is that Yahoo's spam blocker is better than those from most ISP's! And your main personal email address won't be as clogged with spam. Some ISPs, like AOL and BellSouth.net give you multiple email accounts free with your paid service.
- 7. Don't give out any financial information, such as checking account and credit card numbers; and especially your social Security number; on the phone or online, unless you initiate the call and know the person or organization you're dealing with. Don't give that information to any stranger. In general, it is only required for medical providers, banks, mortgages and credit card companies.
- 8. Shred any credit card offers, bank account statements, credit card statements and that you receive in the mail and anything that contains your personal identification information (name, address, social security number, driver's license number, mother's maiden name, or account numbers.) If you don't have a shredder, burn them completely in the fireplace.
- 9. 10. Don't fill out the "win a vacation" and other promotions you see in stores and shopping malls. That will just get you on a junk mailing list and guarantee calls from persistent, high-pressure salesmen.
- 11. Don't pre-print your driver's license, telephone or Social Security numbers on your checks. And in states that want to use your social security number as your driver's license number, insist on another method most allow it.
- 12. Report lost or stolen checks immediately. The bank can block payment on the check numbers that are missing. Also, review new checks you receive, to make sure none has been stolen in transit.
- 13. Store new and cancelled checks, credit card statements, medical bills, anything with confidential information, in a safe place and shred them when you are done with them.
- 14. Guard your Personal Identification Numbers (PINs) for your ATM and credit cards, and don't write on or keep your PINs with

your cards. You should also guard your ATM and credit card receipts. Thieves can use them to access your accounts.

- 15. Be creative in selecting Personal Identification Numbers for your ATM and credit cards, and passwords that enable you to access other accounts. Don't use birth dates, part of your Social Security Number or driver's license number, address, or children's or spouse's names. Remember: If someone has stolen your identity, he or she probably has some or all of this information.
- 16. Don't put outgoing mail in or on your mailbox. Drop it into a secure, official Postal Service collection box. Thieves may use your mail to steal your identity.
- 17. If regular bills fail to reach you, call the company to find out why. Someone may have filed a false change-of-address notice to divert your information to his or her address.
- 18. If your bills include suspicious charges, don't ignore them. Instead, investigate immediately to head off any possible fraud before it occurs.
- 19. Check your credit report regularly. Federal law allows you to obtain one from credit report from each of the 3 major credit reporting agencies per year. See this page for more information.
- 20. There are <u>services online</u>, some free, such as <u>SneakMail</u> that provide you with disposable addresses that can be deleted if they begin to receive spam messages. The disposable email addresses forwards email to a real email address of yours, but the sender can not see this. If you create a unique address for each email newsletter or forum you subscribe to you can discard the address is it gets too much spam and just start using another email address.