# Health Class - **Internet Safety Assignment**

1) What are some of the dangers online ? List 3 and HOW they occur . ( 6 marks )

2) How do you avoid these dangers ? ( 6 marks )

Present your findings in a form of your choice, ( e.g powerpoint, poster , report, or even activity for the class )

You may use the following article to assist you ( from bifaloo.com )

## Online Scams & Dangers, And To Avoid Them

### (How To Keep Your Parents & Children Safe from the Internet)

If you grew up using a typewriter instead of a mouse this article is for you...

Or, if you know someone new to the internet, please pass this along to them. Parents should also pass these important tips on to their kids.

Online scams can potentially harm your credit. Now, there are Identity theft protection services such as LifeLock available to monitor suspicious activity tied to your personal information. I'll be putting together a related guide in the future on identity theft software & services. Stay tuned.

For now, please read over the following guide to avoiding online dangers such as viruses, malware, spyware, hackers and scams.

Internet Safety Tips Topics Covered:

Email Fraud | eBay Safety | Password Safety

Internet Safety Resources | Kid & Internet Safety

Common Online Scams and Internet Dangers:

### Tips for avoiding Email Scams:

If an email seems too good to be true -- it usually is.

Why would someone in another country randomly choose YOU to give money to? It just doesn't make sense.

- Unless you have connections to royalty, why would all these Prince's be sending you emails? Best just to ignore letters received from so-called Lords, Prince's and other royalty.

- Still not convinced an email is a fraud? Do a check on scam resource sites to see if the sender is a known fraud. (see bottom of page for links).

- New internet users are better off getting a free online email account (gmail, yahoo, hotmail, etc.) rather than one that downloads emails onto their computer directly (such as MS Outlook).

- Use Gmail for email. It is free, made by Google and has far better spam filters than other alternatives. My friends and relatives: Please use Gmail, then I won't have to come over to your house and fix Outlook for you...again.

## Common Email Frauds - Spotting Nigerian Scams, Fake Lottos, etc.

The Nigerian (or 419) scam is a type of advance fee scam in which perpetrators try to trick their victims into giving them money under false pretenses.

Often the victim receives an email about an inheritance they are entitled to. The catch is they must first send a check to the sender for the inheritance tax and other fees. Other examples include fees to extend credit or return checks or offers to sell crude oil at ridiculously low prices.

Please remember not to trust email from anyone you don't know.

## Avoid Email Phishing Scams

In a typical phishing scam, the scammer will send an e-mail that looks like it came from a bank. Other common Phishing schemes send spoof emails pretending to be from Ebay, Paypal or other large internet companies. The e-mail will look official and often include a link to a fake website (that look's like the real thing) for the victim to click and enter personal information or passwords, financial information, etc. Scammers collect this data and use it for identity theft.

Remember: no legitimate financial institution will ever ask for personal or account information via email. Any email that requests such information should be deleted immediately. That is always the "tell" with any phishing scam. No one should ever click on a link in any e-mail that says it is from a bank. It is always best to enter the web address for the financial institution in your Internet browser and do all banking and bill paying from there. Most banks now have trust words or trust icons. Make sure your parents are using a bank with this added security, and make sure that they know not to enter personal information unless they see that trust word or icon.

Eliminate the spam, which will eliminate the "phishing." The best way to do this is to set up mom and dad with two e-mail accounts: The first one should only be used with

Scam Quickies
(for our lazy readers)

Common Themes of Email Scams :
- easy money
- free / cheap products / services
- foreign lotteries

Remember :

- Pay Safely, try to use PayPal, Google Checkout, Escrow.com or your Credit Card which all offer some sort of buyer/seller protection. Avoid wire transfers.

Email Safety:

- Just because an email says it's from Uncle Bob or your bank doesn't mean the bank or Bob is the real sender.

- It's not just about not opening emails from people you don't know -- it's about not opening any attachment you are unsure of (even if it's from a familiar name -- email senders can be "spoofed".

- Your bank will not send you an email requesting sensitive information such as your username, password, account number, etc. Emails asking for this information should be deleted. If you need to access your bank's website; never click on a link from an email to visit the site. Instead always use your browsers address bar to type in the website URL or use your personal bookmark to access the site.

- Get a separate email address to use for all correspondence other than your financial information. Blifaloo recommends Gmail.

trusted sites like financial institutions. The other can be used for personal correspondence and signing up for a MySpace account, survey sites, free samples and coupons, etc. If no one knows this e-mail address, no one can send spam or phishing scams. The trick is to really use it only for the trusted sites.

Your parents may think it's okay to use the secret e-mail account for personal correspondence, but what they may not realize is that once someone enters that e-mail address on a free e-card Web site or if they pass along a forward, their e-mail address will be out there for all to see and attack.

## Avoiding Pop-ups, Unwanted Toolbars, and other Harmful Downloads

Reality Check: The internet is a commercially saturated media. New internet users need to understand that a good chunk of "free software" make a profit in other ways. While some of these methods for earning a profit are legitimate, others are completely fraudulent.

For example: free screensavers and smilies (which advertisements often target inexperienced and older demographics) are often accompanied by unwanted toolbars, spyware, adware or worse: viruses.

I recommend Download.com as a safe place to find free downloads as it is proactive about keeping spyware off their site. You can also read reviews of software you are considering downloading. If a download has something unwanted packaged with it, you will usually find user reviews stating so.

When downloading or installing software (from any source), there will often be an option to install some sort of toolbar or other "bonus". This option will of course be selected by default. Be sure to deselect this check box, so the toolbar will not be installed. When installing anything, be sure to read what is being installed before automatically clicking Yes or Next.

## Choosing Strong Passwords

Strong passwords are at least eight characters in length, though 14 or more characters is ideal. The key to creating a good password is to choose something that is not easily guessed by others. Avoid using any part of your name or special dates (birthday or anniversary) in your passwords.

The best way to create a password is to use a pass phrase and then use the first letter of every word and punctuation. For example, "I hate passwords; they are just too hard!" becomes "Ihp;tajth!", which is a very strong password. To go even further, substitute a good mix of special characters (% or @) or numbers for letters, and vary the capitalized letters in the phrase: "1hp,t@j2H!".

It is also possible to just use the phrase itself, but not all Web sites will support passwords of that length (our previous example would be 41 characters), and they are difficult to type correctly every time. If a Web site limits the use of special characters, spaces, and length of the password, concentrate on varying capitalization and using numbers to substitute for letters.

## Using eBay and Craigslist Safely

Online community classified Craiglist.com & the auction site eBay are fantastic places to find a good deal. But new users must learn a bit about possible scams they might run into on these websites.

For Craigslist -- make a point to only deal with a seller locally. Exchange the check for the product after you test it out. If dealing locally is not applicable, do not use checks or money orders. Use a third party, secure payment system like PayPal. PayPal can reverse a transaction if you file a legitimate claim with them (i.e., you never receive an item or the item was not as described).

For eBay, you should read feedback other buyers have left about a seller. Consider the seller's rating before bidding. (Remember, all bids are binding.) If the seller does not have a rating yet, it could mean that it's the first item he or she has sold, but it could also mean that they set up a new account with which to scam buyers. Always Look at the SHIPPING CHARGES on eBay before making a bid.

Again, avoid dealing in money orders & checks, PayPal is highly recommended as well as Google Checkout. Some credit card companies offer extra online security - check with your credit card issuer.