Sample Questions – Internet Safety: Pitfalls & Dangers

Part I: Good Neighborhoods, Bad Neighborhoods

1. In what way is the Internet like a city? (It contains good places and dangerous places.)
2. Name five different kinds of "bad neighborhood" websites. (those that: make unrealistic claims to entice you into making an unwise purchase; contain illegal or immoral content; try to steal your personal information; contain outrageous, unreliable information; are set up to obtain your email address to barrage you with sales emails later)
3. Have you ever gone to a "bad neighborhood" website? If so, what kind? (Answers will vary.)

Part II: Social Network Sites

1. What is the main downside of social network sites? (What you see on your monitor may not reflect what's in the real world.)
2. How do dangerous criminals use social network sites? (They disguise their identities to target young victims.)
3. What can you do to prevent criminals from using a social network site to target you? (Choose a site that allows you to control who can see your page.)

Part III: Your Words & Pictures in Cyberspace

1. What should you never reveal when posting a blog, using a chat room, sending an I-M or email to an online acquaintance? (your last name, address, phone number, usernames or passwords)
2. Why should you always think twice about posting words and pictures online? (because they can last for many years and be resent to family members, teachers, college admissions officials, possible employers, the police)
3. Why should you consider changing a handle the gives too much information about your identity? (A criminal may be able to find out who you are and where you live.)
4. What should you do if someone sends you an I-M or email that discusses private matters that make you feel uncomfortable? (End the conversation, and tell a parent or other adult.)
5. Why should you never call an online acquaintance? (Your number can be displayed on caller ID; then, using an online reverse phone number service your family's name and address can be revealed.)
6. What should raise a red flag? (an online acquaintance asking you to meet in an out-of-the-way place)
7. What should you do if you meet an online acquaintance? (Meet where there are lots of people around; always bring a parent or friend. Note: it's generally preferable *not* to meet an online acquaintance in person.)

Part IV: Online Shopping

1. What are two things you should look for when on a checkout page? ("https" and a lock icon)
2. What kind of online merchants are generally most trustworthy? (a well-known retailer)
3. What three things should an online merchant have on its web site? (street address, phone number, clearly stated return and refund policy)
4. Is there any way to verify that the merchant web site is trustworthy? (Yes, major browsers and many Internet providers have verification software and indicator icons.)

Sample Questions – Internet Safety: Pitfalls & Dangers, p. 2

Part V: An Internet Email Scam

1. What do criminals who use pfishing schemes try to steal? (credit card and social security numbers, bank account numbers, passwords, etc.)

2. How do pfishing schemes normally begin? (with an email notification that a bank or other financial institution has lost important information)

3. What does a pfishing email ask the recipient to do? (Immediately go to a linked website to solve the problem.)

4. What should you do if you receive a pfishing email? (Delete it.)

Part VI: Cyberbullying

1. What is a cyberbully? (a person who humiliates or harasses classmates or acquaintances through postings on blogs, website guest books, I-Ms, cell phone text messages)

2. Is cyberbullying harmless? Why or why not? (No. It has resulted in suicides, assaults, murder and school expulsions.)

3. Is cyberbullying illegal in our state? In our school district? (Answers will vary.)

4. What should you do if someone cyber-bullies you? (Ignore the messages.)

5. What should you do if you receive a threatening cyberbully message? (Tell an adult – a parent or counselor – or possibly call the police.)

6. Why are most cyberbullies considered immature? (Mature persons don't hide behind a computer.)

Name _____

For Parents: Internet Safety Unit

Dear Parent:

As the Internet plays an increasingly important role in our everyday lives, it has become clear that we must make certain that our children learn to use this resource wisely and safely.

With that in mind, we will start our Internet Safety unit in a few days. The unit will have seven lessons: (1) Good Websites, Bad Websites (2) Social Network Sites; (3) Your Words & Pictures in Cyberspace; (4) Online Shopping; (5) Pfishing Scams; (6) Cyberbullying; and (7) A Unit Review.

I would like to ask for your help in this unit. I have attached a unit outline with this letter. Please look it over and review the information with your child. As the unit title suggests, we will spend a great deal of time discussing how to use the Internet safely. These lessons will be not theoretical. One social network site recently found that approximately 29,000 criminals used its site to target victims. I would encourage you to establish some Internet usage rules that would be appropriate in your household and, if you have not already done so, download blocking programs that will protect your child from inappropriate sites.

Thank you very much for your cooperation.

Sincerely,

Name _____

Unit Overview

I. Lesson One: Good Neighborhoods, Bad Neighborhoods

A. Comparing cities and the Internet

1. Cities have good and bad neighborhoods
2. The Internet has good and bad websites
3. Some neighborhoods are dangerous
4. Some websites are dangerous

B. Dangerous website examples

1. Entice you to make an unwise purchase
2. Attempt to steal your personal information
   a. Credit card numbers
   b. Social security numbers
   c. Bank account numbers
3. Contain illegal or immoral content
4. Try to get your email address to send unwanted email later

II. Lesson Two: Social Network Sites

A. Social network sites are popular, used by millions daily

1. Keep track of friends
2. Make plans
3. Share thoughts
4. Make new friends

B. The downside

1. Dangerous criminals target victims on social network sites
2. Many expert liars who know how to cultivate your trust

C. Cautionary action necessary

1. Chose website carefully
2. Site should allow you to control who can see your page

III. Lesson Three: Your Words & Pictures in Cyberspace

A. Safety Rules for people who post a blog, use a chat room, send instant messages or emails to online acquaintances

1. Never divulge your last name
2. Never reveal your address
3. Never disclose your phone number
4. Never tell usernames or passwords

B. Posting information and pictures wisely

1. Be comfortable with having others see them
2. Consider that online postings can last for many decades, or longer
3. Can be seen by family members, teachers, college admission officials, possible employers, law enforcement officials

C. Online words and pictures may be accessed by criminals

1. Do screen names, handles offer too many clues about your identity?
2. The dangers of sending your picture to online acquaintances

a. Police reports full of examples of victims of stalkers met online
b. May be placing your life in jeopardy

D. Other danger signs

1. Inappropriate emails or I-M messages
2. A request for you to call on the phone
3. A request to meet in an out-of-the-way place

a. Forest preserve
b. Deserted house or apartment

E. Rules for meeting an online acquaintance (always best not to meet)

1. Meet in a place where there are lots of people around
2. Meet during the day
3. Bring along a parent or friend, never go alone
4. If bringing a friend, always tell an adult where you're going and when you will return

IV. Lesson Four: Online Shopping

A. Keeping your parents' credit card number safe

1. Look for "https" in the browser's address window
2. Look for the lock icon

B. Some criminal programmers can forge "s" and lock icon

1. Order from well-known companies
2. Make sure company has street address
3. Make sure company has phone number
4. Be certain it has clearly stated return and refund policy
5. Use only browsers and/or Internet providers that verify sites

V. Lesson Five: An Internet Email Scam (Pfishing)

A. What pfishing is

1. A method Internet criminals use to obtain private information (credit cards, social security numbers, banking information)
2. A way criminals can steal an individual's identity

B. How pfishing schemes work

1. Begins with an email that claims bank or other company, institution has lost important information
2. Urges recipient to act immediately
3. Contains website link
4. Website appears legitimate, but isn't and asks for private information

C. What to do with a pfishing email: delete it

VI. Lesson Six: Cyberbullying

A. Definition of cyberbully: a person who harasses or creates hurtful communication in one or more ways

1. On blogs
2. On website guest books
3. On I-M postings
4. In emails
5. On cell phone messages

B. Cyberbully messages can have unintended consequences

    1. Suicide
    2. Serious assault
    3. Murder
    4. School expulsion

C. Cyberbullying may be illegal

    1. Many states have laws against cyberbullying
    2. Many states are considering similar legislation

D. Cyberbullies tend to be immature

E. What should you do if someone cyberbullies you?

    1. Ignore
    2. Tell an adult and/or call police if serious threat in a cyberbully message

VII. Lesson Seven: Review

Name _____

Beyond "Bad Neighborhood" Sites

As you saw in the video, there are different kinds of "bad neighborhood" websites. But these websites aren't the only online danger. One of the most commonly used devices cybercriminals use to steal information is software known as "spyware." Secretly residing in your computer, some versions of spyware copy your keystrokes and then send this information to the cybercriminal. So when you type in passwords, usernames, bank account numbers and so on, the information is passed on to a person who can then access your various Internet accounts using the data they've stolen. Many people have had their identities pilfered by criminals who use spyware.

Identity theft is a major problem. In a recent year, 15 million people were victims of this crime and losses in the United States alone were estimated at more than 56 billion dollars. Identity theft victims may spend many months trying to straighten out the mess left by criminals who may clean out their bank accounts, run up massive charges on their credit cards and wreak other kinds of havoc with their ill-gotten information. The best way to foil cybercriminals who use spyware is to install an anti-spyware program on your computer. There are many such programs commercially available. Some Internet providers offer spyware for free.

Spyware is only one kind of malicious software, commonly called "malware," that can cause serious problems on your computer. Other kinds of malware include viruses, worms, and Trojan horses. Without your knowledge, these programs can use your computer to engage in criminal activity. They also can slow down your computer's operation or even destroy its contents. Antivirus software should be used to make certain these kinds of malware don't infect your compu- ter. There are several excellent anti-virus programs available for free online.

All major computer operating systems come with programs called "firewalls" to keep malware out of your computer. If a person makes certain that his or her computer has active firewall, spyware and virus protection software – and if all these programs are set to automatically update themselves – the computer probably will never be infected. Or if it is infected, the programs will be able to isolate the malware so it won't work on the computer.

Cybercrime is a growing international problem. Large cybercrime organizations are located in Romania, Russia, China, Africa and elsewhere. They use malware to target victims throughout the world.

If you have a home computer, check to see if it has anti-virus and anti-spyware programs on it. If you have a PC, left click the start button and click the "all programs" button to conduct your search. If you have a Mac, click the startup drive icon on the desktop, then click "applications." Report back to class with the names of the anti-malware programs installed on your home computer.

Name _____

Am I Safe?

Directions: Check the items below if they properly describe your online practices.

- ☐ 1. If I have a social network page, I use a site that allows only known friends to access my page and I don't allow anyone else to see it.
- ☐ 2. I never divulge my last name to online acquaintances.
- ☐ 3. I never reveal my address to online acquaintances.
- ☐ 4. I never disclose my phone number to online acquaintances.
- ☐ 5. I never tell my usernames or passwords to online acquaintances.
- ☐ 6. My handles don't offer any clues to my identity.
- ☐ 7. I've never sent my picture to an online acquaintance, and don't plan to.
- ☐ 8. I've never met an online acquaintance in person, and don't plan to.

If you checked 7 or more items, you are safe. If you checked 5-6 items, you may be placing yourself in danger. If you checked fewer than 5 items, you are unsafe. If you checked fewer than 7 items, you should consider changing your online practices. In the space below, state how you can improve your Internet safety.

Name _____

Online Purchase Checklist

Directions: Check the items below if they properly describe your online shopping practices.

- ☐ 1. When shopping online, I look for “https” in the browser address window.
- ☐ 2. When shopping online, I look for the lock icon on the browser page.
- ☐ 3. When shopping online, I order only from well-known companies.
- ☐ 4. When shopping online, I make certain the company has a street address.
- ☐ 5. When shopping online, I make certain the company has a phone number.
- ☐ 6. When shopping online, I make certain the company has a clearly stated return and refund policy.
- ☐ 7. When shopping online, I use only a browser and/or Internet provider that verifies the site as “safe.”

If you checked all 7 items, you are safe online shopper. If you checked 5-6 items, you may not get what you’ve ordered. If you checked fewer than 5 items, you’ve significantly decreased your chances of getting what you’ve ordered. In the space below, state how you can improve your online shopping procedures.

Name _____

Avoiding Online Scams

As you saw in the video, "pfishing" is a commonly used scam perpetrated by online criminals. But there are certainly many others.

Many are seen every time there is a natural disaster, such as a major hurricane or earthquake. Immediately, websites appear that ask for donations for disaster victims. But many of these websites are set up by cybercriminals. The best way to avoid becoming a victim of these fake sites, many of which steal not only donated money but also credit card numbers, is to stick to major relief organizations such as the Red Cross if you want to make a donation to help disaster victims.

Online auction fraud is still another kind of scam to which millions have fallen prey. Victims buy something, but the purchased item never arrives. If you buy something on an online auction site, such as eBay, you should check out the seller. EBay and many other major auction sites let buyers rate sellers. You should stay away from sellers who aren't rated, or who have bad ratings. And you should stay away from auction sites that don't rate sellers.

A scam similar to auction fraud is known as the "Congratulations! You've Won…" swindle. You receive an email that informs you that you've won a terrific prize, such as a digital music player, game console or large flat screen TV. You're directed to a website where you're asked to pay for "only shipping and handling charges," usually a few dollars. You pay these "nominal fees" with your credit or debit card. Of course, the free prize never arrives, and your credit or debit card is charged for much more than a "nominal fee." Obviously, you can avoid becoming a victim of this swindle by ignoring these emails.

Some online criminals use postal forwarding and shipping scams that make you unwitting helpers in their unlawful activities. And, at the same time, these swindlers can clean out your bank account. The con works like this: an online ad asks for a "correspondence manager" for an overseas company that doesn't have a U.S. address. The ad says the company needs someone to transfer money to its foreign bank account or to reship goods to its offices. The money and/or goods are stolen. The victim is used to obscure the trail used by police to track down the real criminals. If money is transferred, the criminal learns your bank account number and then cleans out your account.

Another common scam is known as the "Nigerian 419 letter." Research this swindle online and write a brief report telling how it works.

Name _____

Internet Safety Review Outline

Directions: Fill in the blank spaces in the outline.

I. Lesson One: Good Neighborhoods, Bad Neighborhoods

A. Comparing cities and the Internet

1. Cities have good and bad neighborhoods
2. The Internet has good and bad websites
3. Some neighborhoods are dangerous
4. Some websites are dangerous

B. Dangerous website examples

1. Entice you to make an unwise purchase
2. Attempt to steal your personal information
   a.
   b.
   c.
3. Contain illegal or immoral content
4. Try to get your email address to send unwanted email later

II. Lesson Two: Social Network Sites

A. Social network sites are popular, used by millions daily

1.
2.
3.
4.

B. The downside

1.
2.

C. Cautionary action necessary

1. Chose website carefully
2.

III. Lesson Three: Your Words & Pictures in Cyberspace

A. Safety Rules for people who post a blog, use a chat room, send instant messages or emails to online acquaintances

1.
2.
3.
4.

B. Posting information and pictures wisely

1.
2.
3.

C. Online words and pictures may be accessed by criminals

1. Do screen names, handles offer too many clues about your identity?
2. The dangers of sending your picture to online acquaintances

a.
b.

D. Other danger signs

1. Inappropriate emails or I-M messages
2. A request for you to call on the phone
3. A request to meet in an out-of-the-way place

a.
b.

E. Rules for meeting an online acquaintance (always best not to meet)

1.
2.
3.
4.

IV. Lesson Four: Online Shopping

A. Keeping your parents' credit card number safe

1.
2.

B. Some criminal programmers can forge “s” and lock icon, so…

1.
2.
3.
4.
5.

V. Lesson Five: An Internet Email Scam (Pfishing)

A. What pfishing is

1.
2.

B. How pfishing schemes work

1.
2.
3.
4.

C. What to do with a pfishing email:

VI. Lesson Six: Cyberbullying

A. Definition of cyberbully: a person who harasses or creates hurtful communication in one or more ways

1.
2.
3.
4.
5.

B. Cyberbully messages can have unintended consequences

1.
2.
3.
4.

C. Cyberbullying may be illegal

1. Many states have laws against cyberbullying
2. Many states are considering similar legislation

D. Cyberbullies tend to be immature

E. What should you do if someone cyberbullies you?

1.
2.

Name _____

Internet Safety Unit Evaluation, Page 1

Part I

Directions: Put a "T" next to all true statements and an "F" next to all false statements.

___ 1. Illegal websites are an example of "good neighborhood" sites.

___ 2. A "bad neighborhood" site may contain unreliable information.

___ 3. Some websites are set up to obtain your email address.

___ 4. Government regulations prohibit websites from making unrealistic claims.

___ 5. Most websites, like most neighborhoods, are perfectly fine.

Part II

Directions: Circle the letter next to the statement that best completes the sentence.

1. To be safe, social network sites
    a. require that you follow some precautions.
    b. should never be used.
    c. require your registration.

2. Social network sites allow you to
    a. make plans with your friends, make new friends, apply to colleges.
    b. share your thoughts, order pizza, keep track of friends.
    c. make plans, make new friends, share your thoughts.

3. An important downside aspect of social network sites is that
    a. they are expensive.
    b. they are where dangerous criminals may target victims.
    c. they are confusing for most people to use.

Name _____

Internet Safety Unit Evaluation, Page 2

4. One of the best ways to stay safe on a social network site is to
    a. choose a site that allows you to control who sees your page.
    b. use an anonymous handle.
    c. post your picture.

5. Criminals who go on social network sites
    a. are often petty criminals who are not really dangerous.
    b. never disguise their identity.
    c. are expert liars who know how to cultivate your trust.

Part III

Directions: Fill in the blanks.

1. When posting a blog, using a chat room, sending an instant message or sending an email to an online acquaintance, you should never reveal your _____, _____, _____ or _____.

2. It's best to post only information that you're comfortable having others see because _____ _____.

3. People who can see your online words and pictures many years after they have been put online include _____, _____, _____, _____ and even _____.

Name _____

Internet Safety Unit Evaluation, Page 3

4. You should seriously consider changing any handle that reveals too much about you because _____ _____.

5. Two things you should do if someone sends you an email or IM that discusses private information that makes you uncomfortable are _____ and _____.

6. A criminal may obtain your family's _____ and _____ if you send your phone number.

7. If you meet an online acquaintance in person, you should _____ _____ or _____, meet _____at a place_____ _____.

8. You should never meet an online acquaintance in an _____ place, such as a _____or _____.

9. If you bring along a friend when you meet an online acquaintance, tell an adult _____ and _____.

Name _____

Internet Safety Unit Evaluation, Page 4

Part IV

Directions: Draw a line from the online purchasing situation to the best safety rule.

Situation	Safety Rule
1. Checking out when making purchase	a. Choose browser that verifies retail sites
2. Checking legitimacy of company	b. Check for return and refund policy
3. Item arrives broken	c. Look for "https" in browser address bar
4. Considering making a purchase	d. Look for company with street address and phone number, not just post office box

Part V

Directions: On the back of this paper, give a step-by-step description of how "pfishing" scams work.

Part VI

Directions: Put a "Y" next to all true statements and an "N" next to all false statements.

___ 1. Cyberbullies transmit threats, lies and other hurtful communication.

___ 2. Cyberbullies are usually retaliating for something that's happened outside of school.

___ 3. Cyberbully messages have resulted in murders and suicides.

___ 4. The best thing to do is send a return message to a cyberbully.

___ 5. You should call the police if a cyberbully sends a serious threat.

___ 6. Hurtful cell phone messages are not considered a cyberbully event.

___ 7. Some states have made sending cyberbully messages a criminal offense.

___ 8. Cyberbullies are generally quite mature in their behavior.