Internet Safety: Pitfalls & Dangers

Teacher's Guide
Written by Barri Golbus

Produced
by
Colman Communications
Corp.

Table of Contents

Internet Safety: Pitfalls & Dangers

Grades 6-8

Viewing Time: 16:45

PROGRAM OVERVIEW

Intended Audience and Uses

Internet Safety: Pitfalls and Dangers has been produced for junior high and middle school students. It presents crucial information regarding the most common safety issues for youngsters who use the Internet. Teachers may use the video as both introductory and review media for their instructional programs on the Internet. In addition, the program and its ancillary print material may be used as a mini-unit that contains seven distinct lessons: (1) *"Bad Neighborhood" Websites;* (2) *Social Network Sites*; (3) *The Dangers of Placing Personal Information and Pictures on Blogs, Chat Rooms, Instant Messaging, and Email*;

(4) *Online Shopping*; (5) *"Pfishing" Schemes*; (6) *Cyberbullying*; and (7) a review.

A cautionary note: because computer technology and the Internet are both dynamic in nature, the producers have taken special care to stress fundamentals that do not change. Nevertheless, it is impossible for all information to be completely current. Thus, it will be up to the teacher to update students on any changes that may have occurred since the program's production.

Program Synopsis

The program opens with a comparison of city neighborhoods and websites: some are fine; others may be dangerous. Examples of "bad neighborhood" sites include those established to steal credit card and social security numbers and those with erroneous information. Social network sites are covered next. Viewers are warned that the person they see on their monitors may not reflect reality – who that person *really* is. In fact, one recent study reported that more than 29,000 criminals – expert liars who know how to cultivate one's trust – use a social network site to target victims. The program encourages students to use sites that restrict who can view what they post. The third section of the program extends this information to cover blogs, instant messaging, chat rooms and email. A number of safety rules are suggested, followed by section that explains how online information and pictures can last for decades, thereby possibly influencing the outcome for college applications, job interviews and other future occurrences. A dramatized case study of 14-year-old Lily Mandelli, who emails her picture to a stalker, is given. This section of the program also explains what to do if someone instant messages or emails something about personal matters that makes one feel uncomfortable. And

it warns about telling an online acquaintance your phone number; cautions against meeting an online buddy; and finally gives rules for a meeting, if it does occur. The fourth section discusses how to shop safely online, giving several methods to help make sure a parent's credit card information isn't stolen and the purchased items actually arrive. The next section explains how Internet "pfishing" schemes work so students will know how to avoid them. The sixth section discusses cyberbullying. It defines the term and carefully explains why cyberbully messages can be dangerous, resulting in serious assaults, murder, school expulsions and suicide. The legal aspects of cyberbullying are covered briefly, and viewers learn what to do if they receive a cyberbully message that contains a threat. The final section reviews all the major points covered in the program.

VIEWER OBJECTIVES

After viewing this video and participating in the suggested activities, viewers should be able to do the following:

1. List four examples of "bad neighborhood" websites.
2. Tell how to protect oneself when using a social network site.
3. Write at least five rules to follow when blogging, writing instant messages, emailing and visiting chat rooms.
4. Tell why one should reconsider before placing potentially embarrassing pictures or information online.
5. Explain the dangers of revealing too much personal information to an online acquaintance.
6. Tell what to do if an online acquaintance says something personal that makes you uncomfortable or asks to meet.

7. Name six things one should do when making online purchases.
8. Describe "pfishing" schemes and tell how to avoid them.
9. Define cyberbullying and explain why it can be very dangerous.
10. Tell what to do if you receive a threatening cyberbully message.

The producers encourage you to make adaptations and changes to the following lesson plan whenever you feel it will enhance your students' learning experiences. Only by tailoring the material to your unique classroom situation will you be able to maximize the educational experience afforded by these materials.

SUGGESTED LESSON PLAN

Viewing Strategies

This program can be employed in three separate ways. First, the video can be shown in its entirety as an introduction and/or review session for students studying Internet safety. Second, teachers may pick and choose various sequences and select ancillary print material to underscore concepts taught in their current unit on Internet safety. The third way is using the program and all ancillary material as a mini-unit composed of seven distinct lessons. Each section of the program presents core concept material for individual lessons. Review questions that can be asked after each segment have been provided in the ***Sample Questions*** blackline master (see below).

Previewing Activities

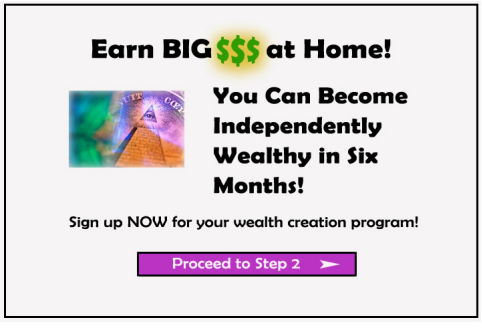
The producers encourage you to prescreen the program to familiarize yourself with its content.

Ask your students how much they use the Internet. In what ways do they use it? For communicating, doing homework, playing games? What websites do they visit most often? Why do they go to those sites? If you are using this program as a mini-unit, duplicate and hand out the ***Unit Overview*** (see blackline masters) and review the outline with your students. Also, if you feel it is appropriate, hand out ***For Parents: Internet Safety Unit*** and instruct your students to take this handout home.

Introduce the Video

Part 1: Good Neighborhoods, Bad Neighborhoods

If you are using this program as a mini-unit, have everyone start an Internet safety folder. As your students work through the unit, have them place all written activities in the folder. Now, tell the class they are going to see a video on Internet safety. Explain that the first segment of the program compares the Internet with city neighborhoods.

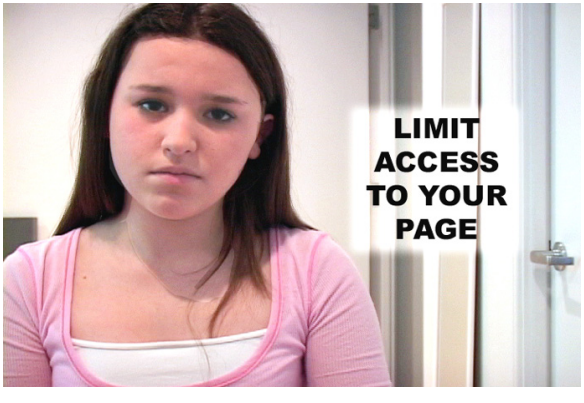


Ask, "Can anyone think how that comparison might be made? In what ways might city neighborhoods be like the Internet?" After exploring these questions, show the first segment.

Post-Viewing Activities

Part 1: Good Neighborhoods, Bad Neighborhoods

Review the kinds of "bad neighborhood" sites mentioned in the program. Those that: (1) try to entice you to make an unwise purchase; (2) try to steal your personal information, such as social security and credit card numbers; (3) contain illegal or immoral content; (4) have unreliable information; (5) try to get your email address to barrage you later with unwanted email. Ask the class if anyone has ever visited an unsafe website. What happened? Did they get unsolicited email? Did they get a large number of pop-up messages that couldn't be closed? Pass out ***Beyond "Bad Neighborhood" Sites***. Have your students read the information and then assign them to identify the anti-malware programs on their computer(s) at home.



Pre-Viewing Activities

Part 2: Social Network Sites

If you feel it would be helpful, review the information presented in the first part of the program. Ask the class how many have a page on one or more social network sites. Discuss how the sites are used. Has anyone ever considered that social network sites can be dangerous? Tell the class

that the next section of the program will explain the dangers of social network sites and how to avoid those threats.

Post-Viewing Activities

Part 2: Social Network Sites

If you feel it is appropriate, discuss in more detail the criminals who use social network sites to target youngsters as victims. Explain that many of these criminals have one or more severe psychological disorders and communicating with them can be extremely dangerous, especially if they are able to find out who you are and where you live. Now ask how many in the class who use social network sites restrict access to their page. If there are any who do not restrict access, show them how to do it (or have a classmate show them) in your school's computer lab if your school allows Internet access to social network sites. If not, ask for volunteers to show or explain how to restrict access elsewhere. Discuss emotional attachments, and their dangers, that can be formed online. Finally, have each student begin a fictional account of someone who became emotionally attached to an online acquaintance and who later came to regret the attachment. *The story should not be completed. The outcome will be written after viewing the next section of the program.*

Pre-Viewing Activities

Part 3: Your Words & Pictures in Cyberspace

If you feel it would be helpful, review the information presented previously. Ask if anyone has ever considered that what they write in an email, on a blog, in an I-M or chat room posting – or the pictures they may place online – can last virtually forever. What are the implications of words and pictures lasting a person's lifetime, and beyond? Mention that many colleges now screen online information posted by applicants on social network sites, blogs and elsewhere. In addition, many businesses do the same thing.

What about putting information in cyberspace that provides personal information to millions of people? Is that a sensible thing to do? Is it prudent, given what was seen in the last part of the program? Finally, explain that the next part of the program will cover some safety issues and will give some advice on how to handle your words and pictures in cyberspace.

Post-Viewing Activities

Part 3: Your Words & Pictures in Cyberspace

Hand out ***Am I Safe?*** Have everyone complete this exercise. After it has been filled in, discuss each item with the class, and then have everyone place it in their Internet Safety notebook if you are using this program as the basis for a mini-unit. How many people were completely safe? Does anyone feel that his or her I-M screen name, chat room handle or blog ID gives too much information about his or her identity? Has anyone ever sent his or her picture to an online acquaintance? If anyone has ever had an unfortunate experience with an online acquaintance, have that individual tell what happened (carefully monitor this discussion to make certain that it doesn't become inappropriate). Be sure your class understands why it is so dangerous to give an online acquaintance your phone number. Has anyone ever met an online acquaintance in person? Underscore what was mentioned in the second part of the program: "…these criminals are **expert liars who know how to cultivate your trust.**" Now, using the information learned in the third part of the program, have your students revise and finish the story they began previously. The story should illustrate the dangers discussed. After the stories have been completed,

have your students read them to the class and then discuss. Finally, have your students put their stories in their Internet Safety notebook if they are keeping one.

Pre-Viewing Activities

Part 4: Online Shopping

If you feel it would be helpful, review the information presented previously. Ask the class how many make online purchases. What things do they buy? Music downloads? Games? Clothing? Explain that most online purchases are made without a hitch, but sometimes things don't go quite so smoothly. Tell the class that the next part of the program discusses how to make certain that online purchases don't go awry. Ask the class to pay close attention to the various strategies discussed that help prevent criminals from stealing credit card numbers and other information.

Post-Viewing Activities

Part 4: Online Shopping

Pass out ***Online Purchase Checklist***. Have your students complete this exercise, then go over their results. How many do everything on the checklist? Have your students put this completed handout in their Computer Safety notebooks. Has anyone ever made an online purchase and then never received the merchandise? What did they do? Did they have any recourse? Has anyone ever heard of a credit card number being stolen while making an online purchase? You might want to mention that, in addition to major browsers and Internet providers, some software companies that specialize in Internet security have free downloadable programs that tell whether a website is safe or not.

Pre-Viewing Activities

Part 5: An Internet Email Scam (Pfishing)

If you feel it would be helpful, review the information presented previously. Write "pfishing" on the chalkboard or on the overhead projector so students can see how the word is spelled. Ask if anyone has ever heard of "pfishing" scams. Can anyone define the term? Explain that the Internet has provided a unique opportunity for criminals to steal credit card numbers and other valuable personal information. Does anyone in the class know a person who has been a victim of online theft? If so, have he or she tell what happened.

Post-Viewing Activities

Part 5: An Internet Email Scam (Pfishing)

Ask the class to review the steps taken by online criminals who use "pfishing" scams to steal personal information. Make certain that the chain of events is clearly understood: (1) an email notification in a person's inbox that appears to be from a legitimate source, (2) a message that claims important information has been lost and that it is urgent that the recipient act immediately, (3) a link to take the recipient to a website that will solve the problem, (4) a legitimate-looking website that asks for various types of information, such as social security numbers, account numbers, passwords, usernames, birth dates and so on. Pass out ***Avoiding Online Scams***. Have your students complete this as a class activity. If possible, invite a local law enforcement official to talk to the class about pfishing scams and other online criminal activity. After the talk, have each

student write a newspaper article detailing what the official said. If your students are keeping an Internet Safety notebook, have them place the article in it.

Pre-Viewing Activities

Part 6: Cyberbullying

If you feel it would be helpful, review the information presented previously. Make certain that your class knows what a cyberbully is (a person who may create blogs, web-site guest books, emails, I-M postings, cell phone messages

or pictures that spread lies, transmit threats, or other harmful, hurtful communication). Tell the class that they may be surprised to learn that cyberbullying may be illegal and may result in events that go far beyond the cyberbully's original intent. Tell the class they will now see a section of the video that discusses cyberbullying and its many unintended consequences.

Post-Viewing Activities

Part 6: Cyberbullying

Discuss the statement "It's rare for older teens to be cyberbullies. They've outgrown the childish behavior that entails hiding behind a computer." Help your students understand that mature individuals don't spread false information or rumors, and they certainly don't do so anonymously. Now, turn your attention to what one should do if he or she is the victim of a cyberbully attack. Why is ignoring the cyberbully a good way to deal with the problem? (Cyberbullies look for a response.) Why is it important to tell an adult if a cyberbully message contains a

serious threat? (The cyberbully may be capable of carrying out his or her threat.) Next, have your students conduct an online search to determine the criminality of cyberbullying in your state. Have them write a brief report on your state's laws, if any, regarding cyberbullies. Discuss the reports and have your students place the report in their Internet Safety notebooks if they are keeping one. Finally, invite a local law enforcement official to your class to discuss cyberbullying. As before, have your students write a report that summarizes the official's presentation.

Program Review

Part 7: Review

If you have used this program as a mini-unit, have your students read over their unit notebooks and ask if they have any questions on any of the material. Hand out the ***Internet Safety Review Outline*** if you have not already done so. Have your students complete this exercise as individual seatwork, in small groups, or as an oral class activity. After the review session, have you students review all the material in their Internet Safety unit notebooks. Finally, pass out the ***Internet Safety Unit Evaluation.*** Have the class complete this evaluation and use it as a key factor in determining a unit grade.

Description of Blackline Masters

SAMPLE QUESTIONS – Provides teachers a set of questions to ask after each segment of the program has been shown.

FOR PARENTS: INTERNET SAFETY UNIT – A letter to parents that explains the unit and asks for their support to help make the unit a success.

UNIT OVERVIEW – Helps parents and students understand the scope and sequence of the unit.

BEYOND "BAD NEIGHBORHOOD SITES – Provides information on various kinds of malware and cyber crimes not discussed in the video.

AM I SAFE? – Reviews safety rules by providing a checklist for students to use when determining whether their online practices are safe or unsafe.

ONLINE PURCHASE CHECKLIST – Reviews safe online purchasing practices and gives students a chance to determine whether or not their online purchasing practices are safe.

AVOIDING ONLINE SCAMS – Gives students an overview of the most common online scams not covered in the video.

INTERNET SAFETY REVIEW OUTLINE – Gives students an opportunity to review the key concepts presented in the program.

INTERNET SAFETY UNIT EVALUATION – An evaluation exercise that will help you and your students determine how much they have learned from the seven lessons presented.

ANSWER KEY

Video Quiz: 1. True 2. Any three of the following: never tell your phone number; change any of your handles if they give too many clues about your identity; limit access to your social network page; never email your picture to an online acquaintance; never call an online acquaintance. 3. c. 4. False 5. Her handle revealed too much information about herself and/or she emailed her picture to an online acquaintance 6. Because the number can be displayed on caller ID, and then a person's name and address can be revealed through an online reverse phone number service 7. Lots of people around, friend, parents 8. c. 9. False 10. Talk to a parent or school counselor, contact the police

Beyond "Bad Neighborhood" Sites: Answers will vary.

Am I Safe?: Answers will vary

Online Purchase Checklist: Answers will vary.

Avoiding Online Scams: Answers will vary.

Internet Safety Review Outline: **IB2a-c**: credit card numbers, social security numbers, bank account numbers **IIA1-4**: keep track of friends, make plans, share thoughts, make new friends **IIB1-2**: dangerous criminals target victims on social network sites, many are expert liars who know how to cultivate your trust **IIC2**: site should allow you to control who can see your page **IIIA1-4**: never divulge your last name, never reveal your address, never disclose your phone number, never tell usernames or passwords **IIIB1-3**: be comfortable with having others see what you've posted, consider online posting can last for a long time (decades or more), postings can be seen by family members, teachers, college admission officials, possible employers, the police **IIIC2a-b**: forest preserve, deserted house or apartment **IIIE1-4**: meet in a place where there are lots of people around, meet during the day, bring along a parent or friend (never go alone), if bringing a friend, always tell an adult where you're going and when you plan to return **IVA1-2**: look for "https" in the browser's address window, look for the lock icon **IVB1-5**: order from well-known companies, make sure the company shows its address, make sure the company shows its phone number, make sure the company has a clearly stated return and refund policy, use only browsers and/or Internet providers that verify sites **VA1-2**: a method Internet criminals use to obtain private information (credit cards, social security numbers, banking information), a way criminals can steal an individual's identity **VB1-4**: begins with an email that claims a bank or other institution has lost important information, urges recipient to act immediately, contains a link to a fake website, website asks for private information **VC**: delete it **VIA1-5**: on blogs, on website guest books, on I-M postings, in emails, on cell phone messages **VIB1-4**: suicide, serious assault, murder, school expulsion **VIE1-2**: ignore, tell an adult and/or call police if serious threat in cyberbully message

Internet Safety Unit Evaluation

Part I 1. F 2. T 3. T 4. F 5. T
Part II 1. a. 2. c. 3. b. 4. a. 5. c.
Part III 1. last name, address, phone number, usernames and passwords 2. it can last for decades or longer 3. family members, teachers, college admission officials, possible employers, police 4. a criminal might figure out who you are and where you live 5. end the discussion, tell an adult (parent) 6. name, address 7. go with a friend, parent, during the day, with lots of people around 8. forest preserve, deserted house or apartment 9. where you're going, when you'll return
Part IV 1 to c, 2 to a or d, 3 to b, 4 to a or d

Part V (1) email that says information is lost and (2) urges immediate action through (3) a linked website that (4) asks for private information
Part VI 1. Y 2. N 3. Y 4. N 5. Y 6. N 7. Y 8. N

TRANSCRIPT OF THE VIDEO

Part I: Good Neighborhoods, Bad Neighborhoods

NARRATOR: If you travel around any large city, you'll probably find a rich variety of neighborhoods.

Some may have expensive homes on tree-lined streets; others may be nice, but not quite so exclusive.

Still others may be extremely dangerous – places you undoubtedly would never want to visit.

The Internet, at least in one respect, is a lot like those cities. While most websites, like most neighborhoods, are perfectly fine, others are online locations you would be well advised to avoid.

Some of these so-called "bad neighborhood" sites may make unrealistic claims to entice you into making an unwise purchase.

Or their content may be illegal or immoral.

Or their sole purpose may be to steal your personal information, such as social security and credit card numbers. We'll discuss these sites in more detail in a few minutes.

Some other "bad neighborhood" web sites may contain completely outrageous and unreliable information, or may be placed online to obtain your email address in order to barrage you later with scores of unwanted emails that try to sell you something.

Part II: Social Network Sites

Some websites are safe, but *only* if you follow some precautions. Social network sites are notable examples.

If you're one of the millions of people who visit a social network site each day, you know that they're a great way to keep track of friends, make plans, share your thoughts and perhaps make some new friends.

But there *can be* a downside because what you see on your monitor – it's in cyberspace, after all – doesn't necessarily reflect what's in the real world.

In fact, some news accounts have reported that a major social network site uncovered some 29,000 criminals – some extremely dangerous – who disguised their true identity to target victims.

Most of these criminals are expert liars who know how to cultivate your trust.

So clearly, some cautionary action is in order. First, you'll want to limit access to your page to weed out undesirable individuals.

That means choosing a site that allows you to control who can see your page and your information.

PART III: Your Words & Pictures in Cyberspace

Now a few cautionary words if and when you post a blog, use a chat room, or send an instant message or email to an online acquaintance.

Never reveal your last name, address, phone number, usernames or passwords.

Also, it's just common sense to post only information that you're comfortable having others see, because, after all, in the online world it's easy to spread personal information far and wide, to a worldwide audience that potentially numbers in the millions.

You'll want to keep in mind that postings, including those that may seem funny at the time, can last for years, decades, or even longer, because they can be downloaded, saved and then resent in the future – to family members (including parents), teachers, college admissions officials, possible employers and even the police.

So think hard before posting anything that could be embarrassing or harmful to you both now *and* in years to come.

Keep in mind, too, that your online words and pictures may be accessible to individuals whose intentions are far less than honorable.

Thus, an I-M screen name, chat room handle or blog ID that gives too many clues about your identity may pose some serious risks.

If any of *your* handles are too revealing, here's an important safety tip: seriously consider changing them a clever felon might be able to figure out your full name – and more – after reading a few of your emails or blog posts.

For instance, after digging around on the net, he could decipher this screen name as Lily Mandelli, age 14, at Westfield Middle School.

If Lily posts some pictures of herself on her social network website or blog, or if she emails her picture to a person she's met in a chat room, or texted in an I-M session, Lily may be placing herself in mortal danger.

That's right – mortal danger.

Police reports are full of examples of victims who were stalked by an individual they had met online, and then foolishly emailed their picture to that person.

Now, a few more safety tips before we move on: First, if anyone sends you an instant message or email that discusses private matters that make you feel uncomfortable, it's time to end the conversation or correspondence.

And then tell an adult, such as a parent, about it.

Next, if an online acquaintance asks you to call him or her on the phone, it could be dangerous to do so because your phone number can be displayed on caller ID.

Then, using an online reverse phone number service, a criminal can easily track down your family's name and address.

Finally, it's not a good idea to meet an online acquaintance in person.

However, if you do, never meet him or her in an out-of-the-way place, such as a forest preserve or a deserted house – no matter what he or she says.

In fact, any suggestion to meet in an uninhabited place should immediately raise a red flag.

If you do meet, it should be where there are lots of people around. An outside mall during the day would be a good choice.

And always bring along someone – a friend, or preferably, a parent. If it's a friend, tell someone else where you're going and when you plan to return.

But again, as a general rule, it's best to keep an online buddy as a cyberspace friend.

Part IV: Online Shopping

Now let's turn our attention to online shopping.

If your parents let you shop with their credit card to make online purchases, you'll need to make certain that their credit card information isn't stolen.

One of the best ways to do that is, when you're checking out, look at the website address bar at the top of your browser's page.

The address should start with the letters "https" instead of merely "http."

The "s" means the site is "secured" with special software that makes it very difficult to steal any information.

A browser-generated lock icon on most checkout pages normally means the same thing.

However, some criminal programmers have been able to forge the "s" and the lock icon, so you'll need to do more to be certain your credit card information is kept safe.

First, you should make sure that the site is part of a well-known retailer, a company that has a street address – not just a post office box.

In addition, the company's phone number should be posted in case the merchandise gets lost in transit or arrives broken.

Next, check to see that the online store has a clearly stated return and refund policy.

Finally, you should use only browsers such as Internet Explorer, Firefox, Opera and Netscape – or Internet providers, if possible – that verify that you're going to a safe website.

If you don't take all these precautions, there's a better than average chance that you'll never get what you ordered …

Teen: Where's my stuff?

…and your parents' credit card information will wind up in the hands of a criminal scam artist who plies his trade online.

Part V: An Internet Email Scam (Pfishing)

Some Internet criminals specialize in another kind of scam.

They send so-called "pfishing" emails to unsuspecting victims to steal social security numbers, credit card information and other private data that allow them to walk off with their victims' money and personal identities.

More often than not, pfishing schemes start with emails that claim that a bank or other financial institution has lost information on your (or your parent's) account.

They also contain statements that urgently implore you to act immediately.

They generally have a link to what's supposed to be legitimate website that will clear up the problem. But the site is fake, although it may look like the real thing.

It often asks for names on the account, social security and account numbers, passwords as well as usernames, birth dates and so on.

So if you ever get an email like this, the best thing for you to do is delete it.

Part VI: Cyberbullying

While some people use the Internet for criminal activities, others may go online to humiliate or harass classmates or acquaintances.

As you probably know, they're called cyberbullies.

Cyberbullies may create blogs, website guest books, I-M postings and even cell phone pictures and text messages to spread lies, transmit threats, or send other hurtful communication.

Sometimes cyberbullies are retaliating for something that's happened offline, usually at school.

Often, they don't realize the full consequences of what they're doing.

Similarly, some people may think that making fun of others or spreading rumors about them online is entertaining, and won't have any real-world significance.

But they're wrong.

Although rare, some cyberbully events have resulted in suicides, serious assaults, murders and school expulsions.

A number of state legislatures have now passed laws that make some forms of cyberbullying criminal acts. Other states are considering similar legislation.

So clearly, cyberbullying is <u>not</u> all fun and games. Moreover, it's immature.

Most cyberbullies are between nine and 14 years old, according to the latest research.

It's rare for older teens to be cyberbullies. They've outgrown the childish behavior that entails hiding behind a computer.

So what should you do if somebody cyberbullies you? Most experts say that, as a general rule, you should ignore it, difficult as that may be.

If it's an email, block the sender.

Do the same if it's a message on your social network site.

If there's a serious threat in a cyberbully note, talk to a parent or parents, a school counselor – or call the police, difficult as that may be.

PART VII: Review

The Internet, then, can be a great place to learn, communicate with friends and acquaintances, and buy your favorite music or videos – or an unlimited array of other items.

You undoubtedly already know that.

Regrettably, however, the Internet is also a place where undesirable and sometimes dangerous people may hang out.

But if you follow a few safety rules, you can save yourself a lot of grief – and perhaps even your life.

If you want a social network page, place it on a site that allows you to control who can see it.

Never tell an online acquaintance your last name, social security number, address, phone number, usernames or passwords.

Post only information that you feel comfortable with others seeing.

Remember that it's generally not a good idea to meet an online acquaintance in person.

But if you do, make sure there are lots of people around – during the day and in a public place. And bring along a friend or parent.

Be sure your chat room and I-M screen names don't give away your identity.

Be aware of pfishing schemes.

Finally, remember that it's best to merely ignore cyberbullies. But if a cyberbully posts a serious threat, tell an adult about it.

In short, you can have fun, shop and learn a lot on the Internet, if you just exercise a little common-sense caution.

Internet Safety
http://kidshealth.org/parent/positive/family/net_safety.html
Covers the most basics in a clearly and concisely

Stop Cyberbullying
http://www.stopcyberbullying.org/index2.html
An excellent resource to learn more about cyberbullying and how to stop it

Delete Cyberbullying
http://www.ncpc.org/cyberbullying
Another excellent resource from the National Crime Prevention Council

Cybercrime
http://www.symantec.com/norton/cybercrime/index.jsp
Describes the different kinds of cybercrimes, malware, and what to do if you're a victim

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.