Internet Safety

Seminar Lesson Plan and Class Activities

Consumer Action

www.consumer-action.org
221 Main Street, Suite 480
San Francisco, CA 94105
415-777-9635 / TTY: 415-777-9456
info@consumer-action.org

523 W. Sixth Street, Suite 1105
Los Angeles, CA 90014
213-624-8327

Chinese, English and Spanish spoken

Consumer Action created The Internet Safety Training Module in partnership with Microsoft®

Internet Safety Seminar

Seminar Purpose:

To provide workshop participants with an awareness of the risks associated with using the Internet, and knowledge of the tools and practices that users can adopt to keep themselves, their computer data, and their personal information safe while online.

Seminar Objectives:

By the end of the training, participants will understand:

- The potential risks for Internet users.
- The various ways to protect their computers and their data.
- How to protect their privacy from online marketers.
- What parents can do to keep their kids safe online.
- Which tools and practices can enhance their online security.
- Where they can obtain additional information and assistance regarding Internet safety.

Seminar Duration:

This seminar is two-and-a half hours long, with a ten-minute break between sessions.

Materials:

For instructor:

- *Internet Safety: A computer user's guide to privacy and security* brochure
- *Internet Safety Trainer's Manual* (Q&A)
- *Internet Safety* visual teaching aid (PowerPoint presentation with instructor's notes)
- *Internet Safety* seminar materials:
    - Lesson plan (pages 4-8)
    - Activity: *How to Spot a Phishing eMail* (page 9)
    - *How to Spot a Phishing eMail* answer key (pages 10-12)
    - Activity: *12 Tips & Tools for Online Safety* (page 13)
    - *12 Tips & Tools for Online Safety* answer key (page 14)
    - Activity: *Case Studies* (pages 15-18)
    - *Case Studies* answer key (pages 19-21)
    - Evaluation form for the *Internet Safety* seminar (page 22)

You will also need:

- A computer and an area on which to project the PowerPoint presentation
- An easel and pad, or a whiteboard, and markers

For participants:

- *Internet Safety: A computer user's guide to privacy and security* brochure
- Copy of seminar PowerPoint slides (optional)
- Activity: *How to Spot a Phishing eMail*
- Activity: *12 Tips & Tools for Online Safety*
- Activity: *Case Studies*
- Evaluation form for the *Internet Safety* seminar

Seminar Outline

Session One

Welcome	(5)
Risks for Internet Users	(15)
Activity: *How to Spot a Phishing eMail Message*	(15)
Ways to Protect your Computer and Data	(15)
Protecting Your Privacy from Online Marketers	(15)
Break	(10)

Session Two

Activity: *12 Tips & Tools for Online Safety*	(15)
Protecting Your Kids Online	(15)
Activity: *Case Studies*	(30)
Resources	(10)
Questions & Answers	(10)
Wrap-up and Evaluation	(5)

Session One

Instructor's Note: *Before conducting the training, familiarize yourself with the* Internet Safety: A computer user's guide to privacy and security *brochure, the* Internet Safety Trainer's Manual *(Q&A), and the PowerPoint presentation. The PowerPoint presentation contains notes for each slide. These notes offer talking points, and detailed information about the items appearing on the slide. This lesson plan indicates which slide corresponds to each part of the lesson, and when to move to the next one.*

➡**SLIDE #1** (onscreen as participants arrive)

Have participants pick up packets on their way in, or place them on seats/tables before class begins. Direct those participants who arrive early to read the *Internet Safety: A computer user's guide to privacy and security* brochure.

Welcome (5 minutes)

Welcome participants. Introduce yourself and present the purpose of the seminar and the agenda.

You can hand out packets at this point if you have not already done so.

Review the contents of participants' packets. Ask the class to take a look inside their packets and make sure they have all the materials needed.

If it's a small group, you can have participants introduce themselves. Ask the group to tell you what they hope to get out of the seminar. On your whiteboard or easel pad, jot down some of the topics participants want to learn about. You can come back to this at the end of the seminar to make sure you've covered these points. (This activity is designed to serve as a brief icebreaker. It will also give you an idea of what participants' expectations and needs are.)

Risks for Internet Users (15 minutes)

Introduction: Computers, phones and other Internet-connected devices, have become such an integral part of daily life that it can be easy to forget about the risks they pose. While there have been many advances in computer and Internet security, scam artists, hackers and stalkers still find new ways to reach vulnerable targets.

Ask the class, "What kinds of things do you do online?" (Answers might include sending and receiving email, shopping, searching for information, blogging, downloading music, videos, software and other files, and social networking.)

Then ask: "What risks do you take in each of these activities?"

If necessary, prompt participation with the following questions:

- Do you think all your email messages are private?
- Do you think about your online or digital reputation?
- Could someone steal your credit card number during an online transaction?
- Are all the websites you visit safe and legitimate?
- Are you sure none of the files you download contain viruses?

- Are all the people you meet online honest and trustworthy?

Then reveal the next slide.

➡SLIDE #2

Go over each item in the list.

After going through the types of risks, ask, “How do crooks and con artists find their victims online?”

After a moment of participation, reveal the next slide.

➡SLIDE #3

Per slide notes, go over each item in the list.

Activity: *How to Spot a Phishing eMail* (15 minutes)

➡SLIDE #4

Have participants take out the *How to Spot a Phishing eMail* activity from their packets.

This activity can be done individually or in small groups. Instruct participants to circle any “red flags” in the email message and the website text below it—things that might tip them off that the email is phishing for personal information and the website could be “spoofed.”

Allow five minutes to complete the activity.

If the activity was completed individually, invite participants to raise their hands if they would like to point out one of questionable items they found. If the activity was done in groups, rotate among them, giving a spokesperson from each group the opportunity to answer when it is their turn.

Refer to the answer key provided for the list of red flags and additional information.

Ways to Protect Your Computer and Data (15 minutes)

Introduction: A group that monitors Internet crime reported that there were 275,000 complaints and $265 million in losses from Internet scams in 2008. Despite great effort to stop them, crooks and scammers continue to find new ways to commit their crimes.

Ask the class, “What are some things you could do to make your online time safer?”

After a moment of brainstorming, reveal the next slide.

➡SLIDE #5

Per slide notes, go over each item in the list.

Protecting Your Privacy from Online Marketers (15 minutes)

Introduction: While online marketing alone is not a threat, unwanted marketing messages can be a nuisance.

Ask the class, “What are some examples of online marketing that you find bothersome?” (Answers might include pop-up ads, flashing banners, ads that scroll across the web page, and unwanted email offers.)

After a moment of participation, reveal the next slide.

➡SLIDE #6

Per slide notes, go over each item in the list.

Break (10 minutes)

Announce a 10-minute break. Make yourself available for a few minutes to direct people to the restroom or a place to get drinks and snacks.

Leave the following slide onscreen during the break.

➡SLIDE #7

Session Two

Activity: *12 Tips & Tools for Online Safety* (15 minutes)

Introduction: It’s true there are some real risks associated with the Internet. But there are some surprisingly simple ways you can make your online experience much safer.

Introduce the following activity, which helps participants learn about practices and tools that enhance their security online.

➡SLIDE #8

Have participants take out the *12 Tips & Tools for Online Safety* activity from their packets.

This fill-in-the-blanks activity can be done individually or in small groups. Instruct participants to write in the letter of the word or phrase from the list at the bottom of the page that best completes each sentence.

Allow five minutes to complete the activity.

If the activity was completed individually, invite participants to raise their hands to be called on if they would like to read out the correctly completed sentence. If the activity was done in groups, rotate among them, giving a spokesperson from each group the opportunity to answer when it is their turn.

Refer to the answer key provided for the correct responses and additional information to share with participants.

Protecting Your Kids Online (15 minutes)

Introduction: Kids can get a lot out of the Internet, but they can also be at risk online.

Ask, “What do your kids use the Internet for?”
Then, “Are you ever concerned about their online activities?”

After a moment of participation, reveal the next slide.

➡SLIDE #9

Per slide notes, go over each item in the list.

Activity: *Case Studies* (30 minutes)

Have participants take out the *Case Studies* activity from their packets.

➡SLIDE #10

Break the class into four smaller groups. Assign one of the case studies to each of the four groups. Instruct each group to read their case study and then, in response to the question at the bottom of the page, to write down specific recommendations.

Allow 10 minutes to complete the activity.

One by one, have each of the groups read their case study and their recommendations. (Learners can read along and take notes on their own copy from their folders.) After each group is finished, open the floor to the other groups to offer additional recommendations. Use the answer key to check off recommendations that were covered, and to offer those that were missed.

Resources (10 minutes)

Introduction: There are a number of resources that could be helpful if you need more information about using the Internet safely.

➡SLIDE #11

Per slide notes, go over each item in the list.

Questions & Answers (10 minutes)

Preparation: Review the Internet Safety Trainer’s Manual and brochure. The training manual is written in Q&A format to help you answer frequently asked questions.

Open the floor to questions.

Wrap-up and Evaluation (5 minutes)

➡SLIDE #12

Congratulate attendees on their participation in the seminar. Ask them to fill out the seminar evaluation form and leave it on a table or in a large envelope you provide.

Activity: *How to Spot a Phishing eMail*

In the email message and the Web site below, circle any "red flags"—those things that might tip you off that the sender is phishing for your personal information. Be prepared to discuss your choices.

EMAIL MESSAGE

From: Internal Revenue Service (admin@irs.us.gov)
Sent: Thursday, October 08, 2009
To: [your email address]
Subject: IRS Notification—Claim Your Refund

Dear IRS customer,

As of our last review of your tax returns we have determined that you are eligible for a tax refund in the amount of $374.60!

In order to claim your refund, you must submit verification of your identity and mailing address today. If you do not respond by the deadline, your refund will be delayed

To access the clame form for your tax refund, please click here.

As we are committed to your ongoing satisfaction and protection, we will keep all information you provide completely confidential.

thank you
IRS accounts manager

WEBSITE YOU LAND ON AFTER CLICKING LINK IN EMAIL MESSAGE
http://cgi6-secured/irsService/connection_mysql/taxaccounts.irs.com/scam.htm

Tax Refund Claim Form
To claim your refund, please verify your identity and mailing address below.

Name

Mailing Address

Birthdate

Social Security Number

Accessibility | Appeal a Tax Dispute | Careers | Freedom of Information Act | IRS Privacy Policy
©2009. IRS.gov | Internal Revenue Service | United States Department of the Treasury

How to Spot a Phishing eMail Answer Key

Each numbered item is a red flag—a clue that the email and website are phishing. The following pages explain why, and offer tips for avoiding being scammed.

EMAIL MESSAGE

From: Internal Revenue Service **(1)** (admin@irs.us.gov) **(2)**
Sent: Thursday, October 08, 2009
To: [your email address]
Subject: IRS Notification—Claim Your Refund **(3)**

Dear IRS customer, **(4)**

As of our last review of your tax returns we have determined that you are eligible for a tax refund in the amount of $374.60! **(5)**

In order to claim your refund, **(6)** you must submit verification of your identity and mailing address **(7)** today. If you do not respond by the deadline, your refund will be delayed. **(8)**

To access the clame **(9)** form for your tax refund, please click here. **(10)**

As we are committed to your ongoing satisfaction and protection, we will keep all information you provide completely confidential. **(11)**

Thank you,
IRS Accounts Manager **(12)**

WEBSITE YOU LAND ON AFTER CLICKING LINK IN EMAIL MESSAGE

http://cgi6-secured/irsService/connection_mysql/taxaccounts.irs.com/scam.htm **(13)**

IRS.gov **(14)**

Tax Refund Claim Form

To claim your refund, please verify your identity and mailing address below.

Name

Mailing Address

Birthdate

Social Security Number **(15)**

How to Spot a Phishing eMail Answer Key (cont'd)

(1) While a phishing email can come from any source, statistics show that PayPal, the IRS, eBay, and financial institutions are some of the identities most widely used by scammers.

(2) Check the return email address—in this case, typing irs.us.gov into your browser address bar would result in a message telling you the URL (web address) could not be found—proof that the email is not coming from a legitimate source. Since it's possible that the address in the email could lead to a "spoofed" site that looks like the IRS site, it's even safer to find the legitimate IRS web address by doing an online search.

(3) Scammers always use a compelling subject line—something that motivates you to open the email right away.

(4) While some phishing email messages are personalized with your name, many are not. They often are addressed to "member," "cardholder," account holder," or "customer, for example. Another red flag here is that the recipient is addressed as "IRS customer." The IRS, being a federal taxing agency and not a business, does not refer to people as "customers," but as "taxpayers."

(5) Phishing emails typically promise something exciting ("You've won the lottery!") or notify you of a problem ("Your account will be closed!"). These kinds of statements are designed to catch your attention and get you to react immediately and emotionally.

(6) Phishing email messages always require action. In this case, the scammers suggest you must claim your refund (not something the IRS actually requires).

(7) Phishing messages and sites are trying to get usernames, passwords, birthdates, Social Security numbers, credit card numbers and similar types of private information. No legitimate business will ever ask you to provide or confirm this type of sensitive information via email (or instant messaging (IM) or text message). In fact, most companies state clearly in their customer policies that they will never ask for this information in an email.

(8) To get you to react before you have time to think about whether or not the email is legitimate, phishing messages usually set an urgent deadline and threaten a consequence for not acting in time. In this case, your deadline is today, and the consequence of not responding in time is that your refund will be delayed.

(9) Phishing messages often contain misspellings (clame instead of claim, here), bad grammar, awkward language and strange formatting.

(10) There is almost always a link that you are required to click on to get to the page where you must enter your personal information. When receiving a message that you suspect might not be legitimate, never click through to the site from the email or even copy and paste a provided link. Always go to the site of the legitimate business by typing in the web address yourself. Or, call the company directly.

(11) Just in case you might have suspicions about the validity of the email message, the scammers try to assure you they would never do anything to violate your privacy.

(12) This isn't signed with a person's name, and no contact phone number is provided.

(13) After you click the link in the email message, you will be taken to a bogus site set up to look like the real thing. The first clue that this is not the IRS' real site is that the URL doesn't begin with the real IRS homepage address (www.irs.gov). In this case, the difference is obvious. But some scammers try to use a URL that closely resembles the legitimate web address for

the site they are mimicking—like www.citybank.com instead of www.citibank.com, or www.mircosoft.com instead of www.microsoft.com, or www.irs.us.gov instead of www.irs.gov.

(14) Scammers copy the logos, images, fonts and formatting straight from the sites they are mimicking, so don't assume that just because a company's logo or copyright (at the bottom of the page) is on the site that it is legitimate.

(15) Phishing messages and phony sites always ask for one or more pieces of sensitive, personal information.

NOTES:

Scammers now are able to forge the "https://" that you normally see when you're on a secure Web server and a legitimate-looking address. The best defense against this is to type the legitimate address for the business or organization whose site you want to visit into the browser address bar yourself. Do not rely on provided links or URLs.

Scammers can also now forge the little padlock you would normally see near the bottom of the screen on a secure site. To make sure this has not been forged, double-click the lock and check that the security certificate that appears matches the site address. If it doesn't, or if you get any warning messages, leave the site.

Check if your favorite browser offers a tool that warns you if the site you are entering is a known phishing site—some browsers do.

Report phishing email messages or phony websites to the:

- company or organization that is being spoofed
- Federal Trade Commission (FTC) (www.ftc.gov)
- Internet Crime Complaint Center of the FBI (www.ic3.gov)

For more information on phishing, or to report a phishing attempt, visit the Anti-Phishing Working Group online at www.antiphishing.org.

Activity: *12 Tips and Tools for Online Safety*

Fill in the blanks with the correct choices from the list at the bottom of the page.

1. _____ at least once a week will ensure you don't lose a lot of important computer data to a virus or malware.
2. _____ will help you avoid forgetting to update your operating system and software programs manually.
3. You should _____ before selling, donating or disposing of your computer.
4. A(n) _____ in the browser address bar is one way to tell if a shopping site is secure.
5. To confirm a website is authentic, and not a bogus site set up by scammers, _____.
6. It is safest to use a(n) _____ when shopping online.
7. When accessing the Internet on a public computer, you should _____ before leaving.
8. Some attachments and downloads contain _____.
9. Sharing copyrighted materials is _____.
10. _____ are considered by many recipients to be spam, and they sometimes contain a virus.
11. To get rid of a pop-up ad, _____.
12. To avoid getting a lot of spam in your main email inbox, use a(n) _____.

A. setting your computer and software to update automatically

B. double-click the padlock and key icons

C. illegal

D. clear IDs, passwords and other private data

E. a firewall

F. debit card

G. smiley-face icon

H. first change the computer's main password

I. https:// rather than just http://

J. delete your most top-secret files

K. reboot your computer

L. chain letters

M. spam filter

N. backing up your files

O. click the X in the upper-right corner of the window or press ALT+F4 on your keyboard

P. erase your hard drive completely and permanently

Q. credit card

R. read the privacy policy

S. alternate email address for certain activities

T. a good way to save money

U. viruses or unwanted software

12 Tips and Tools for Online Safety Answer Key

1. Backing up your files (N) at least once a week will ensure you don't lose a lot of important computer data to a virus or malware. (**NOTE:** The more frequently you back up, the less data you'll lose if something happens.)

2. Setting your computer and software to update automatically (A) will help you avoid forgetting to update your operating system and software programs manually. (**NOTE:** Most operating systems and software now make it possible to check for updates automatically.)

3. You should erase your hard drive completely and permanently (P) before selling, donating or disposing of your computer. (**NOTE:** Simply deleting files isn't enough. Use built-in "disk cleanup" software or third-party software. Or, you can pay a local computer repair shop to overwrite your files. The computer manufacturer's tech support line may be able to help, too.)

4. An https:// rather than just http:// (I) in the browser address bar is one way to tell if a shopping site is secure. (**NOTE:** The "s" in "https" denotes SSL—secure socket layer—encryption, a way to transmit sensitive information, such as a credit card number, safely. Another thing to look for is a closed padlock or unbroken key in the browser window frame.)

5. To confirm a website is authentic, and not a bogus site set up by scammers, double-click the padlock and key icons (B). (**NOTE:** The site is legitimate if the name in the Web address matches the name on the security certificate that appears onscreen when you double-click.)

6. It is safest to use a credit card (Q) when shopping online. (**NOTE:** The maximum liability for unauthorized charges on a credit card is $50. Liability for unauthorized use on a debit card can be much higher, depending upon when you report the loss. And most debit cards are linked to your bank account, which means a thief could wipe you out, at least temporarily.)

7. When accessing the Internet on a public computer, you should clear IDs, passwords and other private data (D) before leaving. (**NOTE:** Clear sensitive information by clicking on "Tools" at the top of the screen and choosing the appropriate option from the drop-down menu. Or begin by choosing the private browsing option in the browser Tools or Safety menu.)

8. Some attachments and downloads contain viruses or unwanted software (U). (**NOTE:** Open only files that come from a trusted source.)

9. Sharing copyrighted materials is illegal (C). (**NOTE:** It's also risky, since some downloads include unwanted software.

10. Chain letters (L) are considered by many recipients to be spam, and they sometimes contain a virus. (**NOTE:** Check out questionable emails on anti-hoax sites such as www.snopes.com or www.quatloos.com before forwarding them so you don't spread something unwanted.)

11. To get rid of a pop-up ad, click the X in the upper-right corner of the window or press ALT+F4 on your keyboard (O). (**NOTE:** Pop-up ads and banners you click on often become the source of unwanted marketing messages.)

12. To avoid getting a lot of spam in your main email inbox, use an alternate email address for certain activities (S). (**NOTE:** There are many free email services to choose from.)

Internet Safety Case Studies

Internet Safety Case Study 1 (child safety on the computer)

Profile of Dwight Lee:

Dwight Lee, a precocious sixth-grader, recently got his very own computer. It was a gift from his parents, who bought it to help him with his studies when he enters middle school next September.

Dwight loves having a computer of his own; he can be online as much as he wants without his little sister or parents complaining or kicking him off. In fact, most days, Dwight goes straight to his room after school, shuts the door, and gets on his computer.

When his parents ask what he spends so much time doing online, Dwight assures them that he spends most of the time doing his homework, and some of the time talking to "friends" he has made through social networking and game sites. His profile, which he has posted on all the popular social networking sites, includes his favorite songs, a list of his hobbies, and information about where he goes to school. There are also personal photos that Dwight's best friend, Lee, posted using Dwight's password.

Dwight's parents have heard of sites such as Facebook and MySpace and Twitter, but they have never visited them themselves.

One of Dwight's new friends, who he met on a game site, has invited Dwight to meet in person at a local movie theater. He's a little concerned about meeting his new friend alone, but when he suggested meeting at his home, with his parents present, his friend made him feel bad and pressured him to get together someplace private. They are planning to meet next week.

What could Dwight's parents do to create a safer online experience for their son?

Internet Safety Case Study 2 (protecting computer data and personal information)

Profile of Millie and Jose:

Millie and Jose did not grow up with computers—they used typewriters and sent letters by "snail mail." They've just "inherited" their daughter's old computer. Celia thinks her parents will enjoy being able to shop and bank from home, send and receive email, and see the latest pictures of the grandkids.

Celia comes home for the weekend to set up the computer for her parents. Before she leaves Sunday, she teaches them the basics. She tells them she'll be back next weekend to help them with any issues they run into.

Millie and Jose take to the computer like fish to water. In their first week:

- Millie uses the word processing software to type up 27 of her favorite recipes.
- Jose uses his debit card to purchase a fishing rod from a private vendor he came across while "surfing."
- Millie sets up an online banking account. She doesn't want to forget the password, so she makes it Willie, the name of their dog.
- Jose responds to an email requesting his name, address, and credit card information in order to verify a transaction with a major online vendor.
- Millie downloads free songs from a site she found by doing an online search for "free music."
- Millie emails her credit card information to their son so that he can buy a plane ticket home from college for his parents' 35th wedding anniversary.
- Jose responds to an email from a stranger who says she will share her lottery winnings with him if he will help her claim the jackpot.

When Celia returns the following weekend, she realizes she should have given her parents more information and instruction regarding protecting their computer data and personal information.

What could Celia have done before leaving her computer with her parents to help protect their data and personal information?

Internet Safety Case Study 3 (safe and sane social networking)

Profile of Chris Taylor:

Chris Taylor was recently laid off from his job as a teacher at a private elementary school. Over the past two months, he has applied for a number of jobs, but has not received a single call for an interview. He is surprised by the lack of response, since he has nearly 10 years of experience in the classroom and has excellent references from two previous employers.

One of the things Chris has filled his free time with since losing his job is social networking: He has set up an account on all the most popular sites. Chris says the time he spends networking is a good way to connect with old friends, meet new ones, and even find a new job. He has also started a blog, where he posts nearly every day.

One thing that Chris enjoys about social networking and blogging is the opportunity to express himself. In his professional life, he has always felt like he had to keep his opinions, beliefs and thoughts to himself. Now, he frequently writes openly online about his political and religious views, his romantic relationships, and some chronic medical issues he's dealing with.

The only negative experience Chris says he has had online is that one of his new "friends" has been sending messages every day to his personal email address. He's also been calling Chris and leaving unpleasant voicemail messages. (He was able to find his home phone number using information Chris revealed, intentionally or not, online.)

What could Chris do differently to avoid certain consequences of his social networking?

Internet Safety Case Study 4 (file-sharing and using a public computer safely)

Profile of Gin and Lena:

To save money, college roommates Gin and Lena share a computer. They both keep their personal files—from homework and music to movies and tax returns—on the computer's hard drive.

Occasionally, Gin and Lena both need to use the computer at the same time. When that happens, the women take turns going to the university library and using one of the "public" computers available for students. While on the library computer, Gin not only does her homework, she also sometimes shops for books or clothes, purchases airline tickets to go home for holidays and vacations, and pays bills. She often checks and updates her social networking pages, too.

Gin and her roommate are the artsy types: Gin is in a band and Lena is into digital photography. They both use P2P (peer-to-peer) file-sharing services on their shared computer to get their songs and photos out to friends and the public.

Recently, Gin became a victim of identity theft: Someone used her credit card number and her Social Security number to make online purchases and open new credit accounts. She doesn't know how her information was stolen.

How might Gin's personal information have been stolen, and how could she and Lena better protect themselves?

Answer Key for Case Studies

Case Study 1:

What could Dwight's parents do to create a safer online experience for their son?

- Place the computer in a common area rather than allow Dwight to use it in a closed bedroom.
- Set and post clear rules about Internet use, including what Dwight is allowed to do online and which sites he can and can't visit.
- They should also use special software to monitor Dwight's Web activity.
- Limit Dwight's computer use—particularly entertainment and socializing—to what they consider a healthy and reasonable amount of time per day.
- "Friend" their son on all the social networking sites he uses so that they can view Dwight's profile on each site and see who is communicating with him.
- Discuss what information is appropriate to share and what information Dwight should keep private. Let Dwight know it's not okay to share his passwords for social networking and other sites with friends.
- Explain that it's not okay to go alone to see someone he "meets" on the Internet.
- Make sure Dwight understands that he must let them know about any threatening or inappropriate communication.
- Report harassment and predatory behavior to the proper authorities, which may include school officials, local police, or the CyberTipline (www.cybertipline.com or 800-843-5678).

Case Study 2:

What could Celia have done before leaving her computer with her parents to help protect their data and personal information?

- She should have taught her mother how to back up her recipes and other files onto a CD or a flash drive so that she wouldn't lose all her work if the hard drive crashed or the computer were stolen.
- She should have cautioned her parents to patronize only merchants they know and trust; to look for the SSL encryption (https://) in the browser's address bar and a closed padlock or unbroken key in the browser window frame; and to use a credit card—not a debit card—to limit their losses to $50 if their information fell into the wrong hands. (Another option is to use a disposable, or "throwaway," card number offered by some credit card companies. The unique card number good for only one transaction.)
- She should have explained how to create a strong password (use a seemingly random string of letters, numbers and symbols that is at least eight characters long), and to never use something personal, like their pet's name.
- Celia should have warned her parents about phishing emails, such as the one Jose responded to with his credit card information.
- She also should have warned them that free games, music and software downloads sometimes contain viruses and other malicious code. (And, unauthorized file sharing of copyrighted material is illegal.)

- Celia should have let her parents know that it's not safe to send sensitive information via email or instant messaging (IM) on any Web-enabled device (computer, PDA or smart phone).
- She should have made sure the spam filter was set high enough to block the lottery email that her father responded to. And she should have told her parents to delete spam and not respond in any way, even to unsubscribe.
- If Celia's computer is too old to take advantage of the latest security software and hardware (security patches for antivirus software and antispyware, and a functioning firewall, for example), she should have waited until she could provide a newer and safer machine for her parents.

Case Study 3:

What could Chris do differently to avoid certain consequences of his social networking?

- Many employers research job applicants online before interviewing or hiring them. If Chris truly has the experience and qualifications for the jobs he is applying for and he's not getting any responses, it's very likely that his online identity could be holding him back. To be safe, Chris shouldn't post anything on his personal blog or any social networking site that could be considered controversial. Likewise, he should think twice about revealing medical issues that could be of concern to a prospective employer.
- Chris should consider using a pseudonym (a fake name) if he plans to post anything online that he wouldn't want a future employer to see.
- If he does use his real name, Chris should limit the other personal information he reveals, such as his city. The more pieces of his identity he reveals, the easier it is for someone to then get information such as his address and phone number.
- To avoid nuisance email messages, Chris could open a free email account to use specifically for social networking, keeping his regular email inbox clear of unwanted messages.
- Depending on the content of the messages and how many he receives, Chris may be the victim of stalking or harassment. (Each state has its own definition of these crimes.) Chris can report the behavior to local law enforcement. He also can get information, safety tips and resources at the Stalking Resource Center, which is accessible through the National Center for Victims of Crime site (www.ncvc.org.)

Case Study 4:

How might Gin's personal information have been stolen, and how could she and Lena better protect themselves?

- When using the library computers, Gin and Lena should surf "in private," an option offered by many browsers. It means you can browse the Internet without the computer saving any data about which sites you have visited. Look for the "in private" option under the Tools menu or through the Safety button in the top right corner of the window.
- They should never save their logon information on a public computer. When they visit sites that require a password, they should always log out—not just close the browser window—when they are finished or even if they just step away for a moment. If possible, they should disable the feature that stores passwords. (Information is available under the Help tab of the browser.) Or they can clear this info by clicking on the "Tools" in most browsers and then "Delete Browsing History."

- Gin would be smart to wait until she is on her personal computer to shop, buy airline tickets, pay bills, or conduct any other financial transaction online.
- File-sharing allows users to swap personal files stored on their hard drives by making them available on a network (often called a P2P, or peer-to-peer, network). Users can become victims of identity theft when, during set-up, they inadvertently make available to the network their personal files that are in the same My Documents folder as the files they want to share. To avoid such a mistake, some experts advise reserving a separate computer just for file-sharing. If that isn't feasible, either avoid file-sharing entirely, or be extremely careful.
- Even though Gin and Lena trust each other, they should password-protect their personal files; there is always the possibility that a visitor to the dorm room could get on the computer and access their personal files without their knowledge.

Evaluation of the Consumer Action *Internet Safety* Seminar

Before you leave, please help us improve future presentations by giving us your opinion of today's seminar.

Circle the number that reflects your feelings about each statement:

1 = Strongly Agree 2 = Agree 3 = Disagree 4 = Strongly Disagree

I have a better understanding of the potential risks of using the Internet.

1 2 3 4

I have the knowledge I need to better protect my and my family's online privacy.

1 2 3 4

I am more aware of tools, practices and resources that contribute to a safer online experience.

1 2 3 4

The instructor was well informed.

1 2 3 4

The materials I was given are easy to read and understand.

1 2 3 4

The activity contributed to my learning.

1 2 3 4

I would like to attend another class like this.

1 2 3 4

What else would you like to tell us about how we could improve future seminars?

_____

_____

_____