Workshop 3:
Steering Clear of Cyber Tricks
Instructor Handbook

Google

iKeepSafe

Table of Contents

Workshop 3: Steering Clear of Cyber Tricks

Overview:

Students will learn to recognize cyber tricks, scams and phishing attacks. They will understand how to avoid those tricks, how to protect themselves and what action to take if they have been tricked.

The lesson plan can be easily adapted and developed into a more comprehensive lesson or unit. Suggestions for modifications and additional resources are provided.

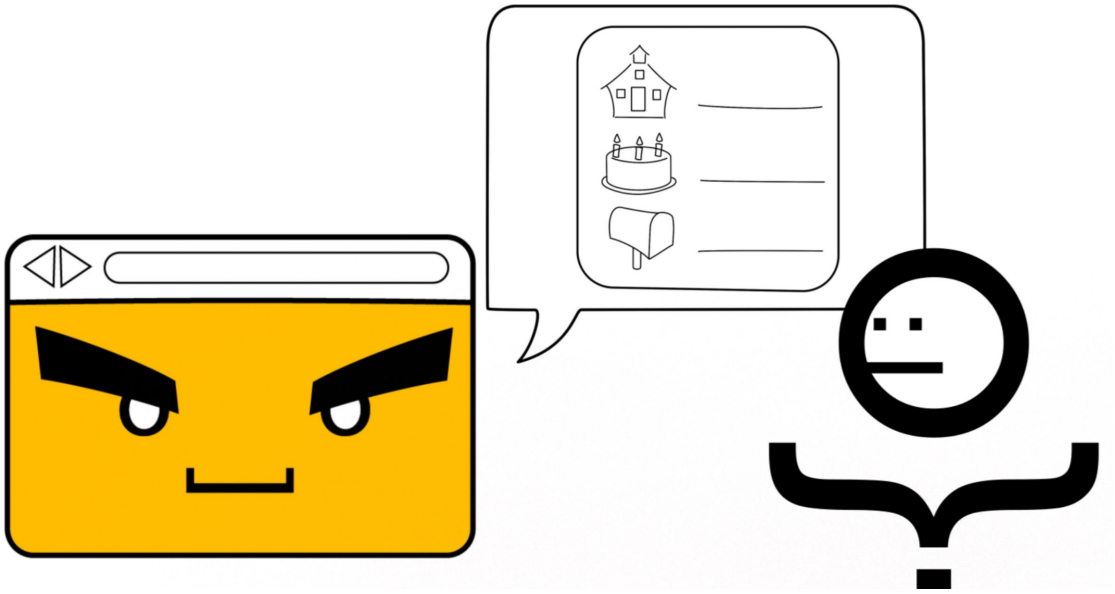
The workshop is accompanied by an Instructor's Toolkit and a Student Handouts booklet.

Lesson plan (approx. 40 min): Steering Clear of Cyber Tricks

Teaching Tips:

Take time to introduce yourself and share a little about your background and your interest in the topic. Next, poll the students to find out what they already know about online behavior. Finally, share a little about what you will be covering – just enough to peak their interest. After the introduction and warm–up keep the momentum going.

1. Make sure your presentation is dynamic and engages the students. "Talking heads" are boring. Make the audience work, calling on different people – male and female.
2. Keep moving so students have something to watch. Try not to get stuck in a corner. Make eye contact with as many students as possible.
3. Research shows that youth respond better to positive rather than negative sets of directions. Use positive rather than negative language. "Craft positive messages and post positive images," is much better received than "Don't post bad things." Reinforce that positive behaviors are the social norm.
4. Limit the amount you read from the board, screen or script. The script is an outline only. Add your own words and character!



Workshop 3
Lesson 1: Steering Clear of Cyber Tricks

Concept: How do you know what you can trust online? What are cyber tricks or scams? How can you avoid tricks and scams? What should you do if you realize you've been tricked by a scam or a phishing attack?

From video: Guidelines to keep yourself safe online from cyber tricks, scams and phishing:

What are cyber tricks/scams?

1. Free offers usually are not free.
    a. If a website asks for financial information to get a free prize, chances are it's a trick.
    b. Some websites trick you into giving them personal information so they can send you more tricks. For example, "personality tests" can be actually gathering facts about you to make it easy, for example, to guess your password or other secret information.
    c. Chain letters may put you at risk. Don't forward them to your friends.
2. To avoid falling for scams, use these tips:
    a. Think before you click.
    b. Stay away from pop-up contests. You can't win and there is usually a secret trick such as collecting information about you, seeing if your email address is active, or infecting your computer with destructive software.
    c. Do a web search for a company's name before you give them any information about yourself.
    d. Read the fine print.
3. Phishing: a scam where an entity tries to steal private information by pretending to be someone that you trust like a friend, your bank or even your email service.
4. To avoid phishing scams, use these tips:
    a. Most legitimate businesses will never ask for personal information like account numbers, passwords and social security numbers via email.
    b. Don't click on any link or file in a suspicious email.
    c. Open a new browser and log into that company's website as you normally would. If there is an issue with your account, the site should give you instructions on how to fix it.
5. If you realize you have been tricked, take action!
    a. Tell a trusted adult immediately.
    b. The longer you wait, the worse it may get.
    c. If you are worried about your bank account or credit card information, contact the bank or credit card company immediately.
    d. If you received a phishing email, go to www.antiphishing.com to report it.

Standards Addressed:

a. ALA Standard 8:3: Student will use information technology responsibly.

b. C3: II:A: Student will recognize online risks, to make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.

c. C3: II:B: Student will make informed decisions about appropriate protection methods and safe practices within a variety of situations.

d. C3: II:C: Student will demonstrate and advocate for safe behaviours among peers, family and community.

e. C3:III:A: Student will recognize online risks, make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.

f. C3:III:B: Student will make informed decisions about appropriate protection methods and secure practices within a variety of situations.

g. C3:III:C: Student will demonstrate commitment to stay current on security issues, software and effective security practices.

h. C3:III: D: Student will advocate for secure practices and behaviors among peers, family, and community.

i. NETS: 5:a: Student will advocate and practice safe, legal and responsible use of information and technology.

Description:

In this lesson, students will receive examples of online scams, learn about the danger, get tips to avoid scams and what actions to take.

General Goal:

- Students will identify online scams and decide what action to take.

Objectives:

1. Students will identify online scams (comprehension).
2. Students will review the dangers of scams (comprehension).
3. Students will select what action to take after detecting a scam, or to avoid a scam (evaluation).

Materials:

- Chart paper or chalk/white board or Smart board.
- Computer with Internet connection and screen projector device for presenter.
- Student Handouts booklet for each student.

Procedures:

1. Start the lesson by asking some questions to determine the students' knowledge. These can be used later as a formative assessment. You can use the questions from Introduction Questions (Instructor Toolkit).
2. Show the students the video by Google, Steering Clear of Cyber Tricks (www.ikeepsafe.org/youtube).
3. Say: "You are going to watch a short video (developed by the team at Google), Steering Clear of Cyber Tricks. This video will explain what cyber tricks are, how to avoid falling for online scams, what Phishing means online (it's not what you think...) and what to do if you realize you have been tricked."
4. Hand out What are Cyber Tricks? (Student Handouts) to the students. Go over the tips with the students.

5. Activity 1 – Online Scams and Phishing Examples

   Tell the students that they are about to see some examples of real Phishing Scams and online Tricks. Hand out Phishing Scams (Student Handouts).

   Say: "In this handout you will see examples of some popular tricks and phishing scams."

   Go over the examples with the students. For each example discuss the dangers, how to avoid falling for that scam and what action to take.

   Highlight these points:
   - Better to be safe than sorry.
   - Always think twice before forwarding something, clicking on something or filling out your personal information.

   Extended activity: Ask the students to play a game at home by counting how many cyber scams they can identify in a week. Tally the results at the end of the week and see who was able to identify the most cyber tricks.

6. Activity 2 – Who Wants to be a Millionaire? A Cyber Security Game

   Let the students know that they are going to play a cyber security game of "Who Wants to be a Millionaire?" to test their knowledge about how to steer clear of cyber tricks. Before you begin, download the PowerPoint file of "Who Wants to be a Millionaire?" You can also prepare your own presentation or use the questions in Who Wants to be a Millionaire? A Cyber Security Game in the Instructor Toolkit. Divide the class into groups of 4-5 students. Each group comes up with an answer and whoever gets it correct scores points. Alternatively, this game can be played in the traditional way where one student is the contestant and the class is the audience.

   Have fun!

Instructor Toolkit

Google

iKeepSafe

Google

iKeepSafe

Workshop 3:
Lesson: Steering Clear of Cyber Tricks

Questions:

- Who uses email in the class?
- Who knows what an online scam is? Give examples.
- Who has received an email scam?
- What should you do when you think you are being scammed? (*Answer: tell an adult, don't click on anything, contact your bank or credit card company and report.*)
- Who is on social networking sites?
- Who has a profile online?
- Is it safe to use your real personal information for an online Avatar? Why? (*Answer: it's better not to reveal too much personal information since this can be used for phishing scams. Don't fill out what you don't need to. You don't need to give your real information. You can open another email and use it for online registrations instead of your personal email.*)
- How can you get an email scam from someone if you never gave your email address to that person? (*Answer: phishing scams use software to "reap" email addresses from other sources, for example, from social networking sites. So if you publish your information somewhere, someone can use it to send you spam and scam emails.*)
- If you get a greeting card from a "secret admirer", should you respond if you don't know who it is? (*Answer: no. If you can't identify a sender, it's better not to click on any links in the email as they can be used to collect your information or to harm your computer.*)
- If you get a chain letter saying that something bad will happen to you or to someone you know if you don't forward it, should you go ahead and forward it to all your friends? (*Answer: nothing bad can happen from not forwarding an email to someone. But forwarding a chain letter may put you and your friends at risk of being tricked or of harming your computer.*)

Google

iKeepSafe

Workshop 3
Lesson: Steering Clear of Cyber Tricks

What are Cyber Tricks?

1. Free offers usually are not free.
    a. If a website asks for financial information to get a free prize, chances are it's a trick.
    b. Some websites trick you into giving them personal information so they can send you more tricks. For example, "personality tests" can be actually gathering facts about you to make it easy, for example, to guess your password or other secret information.
    c. Chain letters may put you at risk. Don't forward to them your friends.
2. To avoid falling for scams, use these tips:
    a. Think before you click.
    b. Stay away from pop-ups contests. You can't win and there is usually a secret trick such as collecting information about you, seeing if your email address is active, or infecting your computer with destructive software.
    c. Do a web search for a company's name before you give them any information about yourself.
    d. Read the fine print.
3. Phishing: a scam where an entity tries to steal private information by pretending to be someone that you trust like a friend, your bank or even your email service.
4. To avoid phishing scams, use these tips:
    a. Most legitimate businesses will never ask for personal information like account numbers, passwords and social security numbers via email.
    b. Don't click on any link or file in a suspicious email.
    c. Open a new browser and log into that company's website as you normally would. If there is an issue with your account, the site should give you instructions on how to fix it.
5. If you realize you have been tricked, take action!
    a. Tell a trusted adult immediately.
    b. The longer you wait, the worse it may get.
    c. If you are worried about your bank account or credit card information, contact the bank or credit card company immediately.
    d. If you received a phishing email, go to www.antiphishing.com to report it.

Google iKeepSafe

Workshop 3
Lesson: Steering Clear of Cyber Tricks

Phishing Scams

1. Email scam (phishing):

Dear Customer,

Sorry for disturbing you, but we have to check your ATM card details.

The management of our bank has made a decision to switch to new transfer security methods because of frequent fraudulent operations. The new updated technologies will ensure the security of your payments through our bank. As both software and hardware will be updated, some personal data will be lost inevitably. In order to restore all information, necessary action should be taken immediately.

We thank you for your cooperation in this manner.

Click below to confirm and verify your Online Banking Account.
https://login.personal.bank.com/verification.asp?d=1

If you choose to ignore our request, you leave us no choice but to temporary suspend your account.

Best Regards, Your Bank
Security and Anti-Fraudulent Department.

Mark everything that applies:

Dangers:

- ☐ Harm your computer by installing viruses, Trojans and other malicious spyware.
- ☐ Identify theft.
- ☐ Steal your money.

How to avoid falling for the scam:

- ☐ Don't open suspicious emails.
- ☐ Don't click on anything.
- ☐ Don't download any attachments.
- ☐ Don't give out any personal information.
- ☐ Don't make any transaction on a site that is not secure. Secure websites have a lock on the bottom right of the browser window. They also start with https://
- ☐ Check to see if the URL matches the authorized website. If it's different, then chances are it's a spoof.
- ☐ Go to the company's website and check for any alerts or information.

What action to take:

- ☐ Tell a trusted adult immediately.
- ☐ Stop all online activity which requires a username, password, or privacy information.
- ☐ Close online accounts if you think they have been compromised.
- ☐ Change passwords and pin numbers.
- ☐ Report to www.antiphishing.com
- ☐ Check if that company has a security center or another place to report phishing scams.
- ☐ Download and install free antiphishing toolbars that protect from some phishing scams.
- ☐ Protect your computer with anti-virus and anti-spam software.

2. eBay Phishing Scam:

Email Subject: Password change required!

Dear sir,

We recently have determined that different computers have logged onto your eBay account, and multiple password failures were present before the log–ons. We strongly advise you to CHANGE YOUR PASSWORD.

If this is not completed by March 8, 2010, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation.

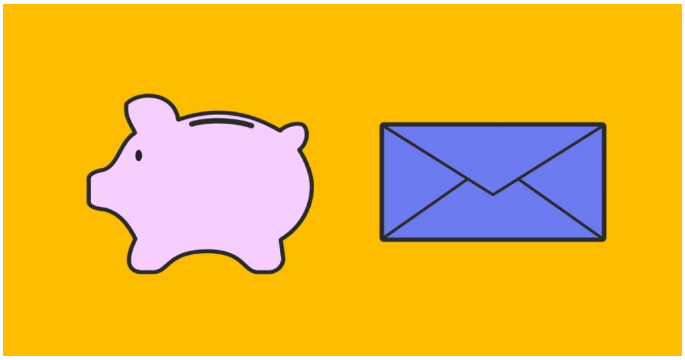
Click here to Change Your Password

Thank you for your prompt attention to this matter.

Mark everything that applies:

Dangers:

- ☐ Harm your computer by installing viruses, Trojans and other malicious spyware.
- ☐ Identify theft.
- ☐ Steal your money.

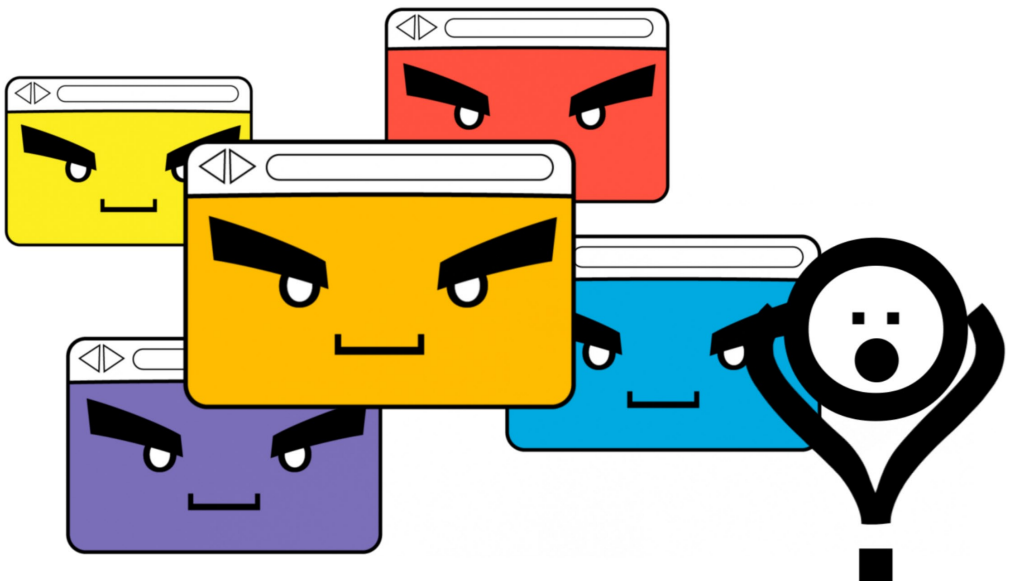


How to avoid falling for the scam:

- ☐ Don't open suspicious emails.
- ☐ Don't click on anything.
- ☐ Don't download any attachments.
- ☐ Don't give out any personal information.
- ☐ Don't make any transaction on a site that is not secure. Secure websites have a lock on the bottom right of the browser window. They also start with https://
- ☐ Check to see if the URL matches the authorized website. If it's different, then chances are it's a spoof.
- ☐ Go to the company's website and check for any alerts or information.

What action to take:

- ☐ Tell a trusted adult immediately.
- ☐ Stop all online activity which requires a username, password, or privacy information.
- ☐ Close online accounts if you think they have been compromised.
- ☐ Change passwords and pin numbers.
- ☐ Report to www.antiphishing.com
- ☐ Check if that company has a security center or another place to report phishing scams.
- ☐ Download and install free antiphishing toolbars that protect from some phishing scams.
- ☐ Protect your computer with anti-virus and anti-spam software.



3. Unsolicited pop-ups:

You surf the web and suddenly get a pop-up that asks you to donate for a charity. They ask for your credit card information.

Mark everything that applies:

Dangers:

- ☐ Harm your computer by installing viruses, Trojans and other malicious spyware.
- ☐ Identify theft.
- ☐ Steal your money.

How to avoid falling for the scam:

- ☐ Don't open suspicious emails.
- ☐ Don't click on anything.
- ☐ Don't download any attachments.
- ☐ Don't give out any personal information.
- ☐ Don't make any transaction on a site that is not secure. Secure websites have a lock on the bottom right of the browser window. They also start with https://
- ☐ Check to see if the URL matches the authorized website. If it's different, then chances are it's a spoof.
- ☐ Go to the company's website and check for any alerts or information.

What action to take:

- ☐ Tell a trusted adult immediately.
- ☐ Stop all online activity which requires a username, password, or privacy information.
- ☐ Close online accounts if you think they have been compromised.
- ☐ Change passwords and pin numbers.
- ☐ Report to www.antiphishing.com
- ☐ Check if that company has a security center or another place to report phishing scams.
- ☐ Download and install free antiphishing toolbars that protect from some phishing scams.
- ☐ Protect your computer with anti-virus and anti-spam software.

4. Unsolicited pop-ups:

You log into a website and suddenly you get a pop-up of an anti-virus that looks like it's scanning your hard drive in real time. There is an enticing offer asking you to click in order to download a free trial of that software.

Mark everything that applies:

Dangers:

- ☐ Harm your computer by installing viruses, Trojans and other malicious spyware.
- ☐ Identify theft.
- ☐ Steal your money.

How to avoid falling for the scam:

- ☐ Don't open suspicious emails.
- ☐ Don't click on anything.
- ☐ Don't download any attachments.
- ☐ Don't give out any personal information.
- ☐ Don't make any transaction on a site that is not secure. Secure websites have a lock on the bottom right of the browser window. They also start with https://
- ☐ Check to see if the URL matches the authorized website. If it's different, then chances are it's a spoof.
- ☐ Go to the company's website and check for any alerts or information.

What action to take:

- ☐ Tell a trusted adult immediately.
- ☐ Stop all online activity which requires a username, password, or privacy information.
- ☐ Close online accounts if you think they have been compromised.
- ☐ Change passwords and pin numbers.
- ☐ Report to www.antiphishing.com
- ☐ Check if that company has a security center or another place to report phishing scams.
- ☐ Download and install free antiphishing toolbars that protect from some phishing scams.
- ☐ Protect your computer with anti-virus and anti-spam software.

5. Greeting cards scams:

It's not even close to your birthday, not a holiday or other occasion, yet suddenly you get a greeting card. It says the following:

Hi my friend,
You have a greeting card waiting for you. Please click here to download.

From your secret admirer.

Mark everything that applies:

Dangers:

- ☐ Harm your computer by installing viruses, Trojans and other malicious spyware.
- ☐ Identify theft.
- ☐ Steal your money.

How to avoid falling for the scam:

- ☐ Don't open suspicious emails.
- ☐ Don't click on anything.
- ☐ Don't download any attachments.
- ☐ Don't give out any personal information.
- ☐ Don't make any transaction on a site that is not secure. Secure websites have a lock on the bottom right of the browser window. They also start with https://
- ☐ Check to see if the URL matches the authorized website. If it's different, then chances are it's a spoof.
- ☐ Go to the company's website and check for any alerts or information.

What action to take:

- ☐ Tell a trusted adult immediately.
- ☐ Stop all online activity which requires a username, password, or privacy information.
- ☐ Close online accounts if you think they have been compromised.
- ☐ Change passwords and pin numbers.
- ☐ Report to www.antiphishing.com
- ☐ Check if that company has a security center or another place to report phishing scams.
- ☐ Download and install free antiphishing toolbars that protect from some phishing scams.
- ☐ Protect your computer with anti-virus and anti-spam software.

6. Lottery scams:

You get an email notifying you that you have just won $650,000! See example below.

Date: Mon, 15 Mar 2004 20:33:38 +0100
From: "johnnewman_ip" <johnnewman_ip@telstra.com>
Subject: INTERNATIONAL PROMOTIONS / PRIZE AWARD DEPARTMENT,
To: maris_n_piper@yahoo.co.uk

DIAMOND LOTTERY.
LEEK ROAD, STOKE ON TRENT
ENGLAND ST1 3NR.

FROM: THE DESK OF THE PROMOTIONS MANAGER,
INTERNATIONAL PROMOTIONS / PRIZE AWARD DEPARTMENT,

REF: EGS/2551256003/03. BATCH: 12/0002/IPD

Attention: Dear Winner,

RE/AWARD NOTIFICATION, FINAL NOTICE

We are pleased to inform you of the announcement of winners of the DIAMOND LOTTERY INTERNATIONAL PROGRAMS UK, held on 29th of October 2003. Your email address, attached to ticket number 111-2465-2000-100, with serial number 3543-07 drew the lucky numbers 12-16-22-39-39-43, and consequently won the lottery in the 3rd category. You have therefore been approved for a lump sum payment of $650,000.00 (Six Hundred and Fifty Thousand United States Dollars) in cash credited to file HWS/200118308/02. This is from a total cash prize of $10,000,000.00 (Ten Million United States Dollars) shared among the seventeen international winners in this category. All participants were selected through a computer ballot system drawn form 250,000 names 300,000 emails from Australia, New Zealand, America, Europe and North America as part of our International Promotions Program, which is conducted annually.

Furthermore, your lucky winning number falls within our Western Europe booklet as indicated in your play coupon. In view of this, your $650,000.00 (Six Hundred and Fifty Thousand United States Dollars) will be paid to you either by our banker or financial agent in London or Spain. Due to a mix up of some numbers and names, we ask that you keep this secret from the public notice until your claim has been processed and your money remitted to your account, as this is part of the security protocol to avoid double claiming or unwarranted taking advantage of this program by participants.

We hope that with part of you prize, you will participate in our end of year high stakes ($1.3 billion) International Lottery. To begin your claim, please contact your claim agent: Jeff Brown, diamondlotteryagent@hotmail.com or my email address for due processing and payment of your prize money.

NOTE: In order to avoid unnecessary delays and complications, please remember to quote your reference and batch numbers in every correspondence. Congratulations again and thank you for being part of our promotion program.

Sincerely yours.
John Newman.
GENERAL MANEGER, INTERNATIONAL PROMOTION PRIZE AWARD DEPT.

Mark everything that applies:

Dangers:

- ☐ Harm your computer by installing viruses, Trojans and other malicious spyware.
- ☐ Identify theft.
- ☐ Steal your money.

How to avoid falling for the scam:

- ☐ Don't open suspicious emails.
- ☐ Don't click on anything.
- ☐ Don't download any attachments.
- ☐ Don't give out any personal information.
- ☐ Don't make any transaction on a site that is not secure. Secure websites have a lock on the bottom right of the browser window. They also start with https://
- ☐ Check to see if the URL matches the authorized website. If it's different, then chances are it's a spoof.
- ☐ Go to the company's website and check for any alerts or information.

What action to take:

- ☐ Tell a trusted adult immediately.
- ☐ Stop all online activity which requires a username, password, or privacy information.
- ☐ Close online accounts if you think they have been compromised.
- ☐ Change passwords and pin numbers.
- ☐ Report to www.antiphishing.com
- ☐ Check if that company has a security center or another place to report phishing scams.
- ☐ Download and install free antiphishing toolbars that protect from some phishing scams.
- ☐ Protect your computer with anti-virus and anti-spam software.

Google iKeepSafe

Workshop 3
Lesson: Steering Clear of Cyber Tricks

Who Wants to be a Millionaire? A Cyber Security Game

For $100:
Q: Cyber tricks and scams come from

A. Criminals
B. Friends
C. Companies
D. All of the above

For $200:
Q: Phishing means

A. Using a phishing pole in the water and catching phish
B. Someone should have been more careful with the spell check
C. Websites and emails created just to trick you so cybercriminals can steal your information
D. All of the above

For $300:
Q: If you suspect you have become a victim of a cybercriminal you should

A. Stop all online activity which requires a username, password, or privacy information
B. Run updated anti-spyware and anti-virus programs
C. Tell a trusted adult
D. All of the above

For $500:
Q: It is fine to open an email attachment before scanning it for viruses if

A. It comes from a friend
B. It comes from a trusted company
C. It comes from your school
D. None of the above

For $1000:
Q: Chain emails are

A. A way to ensure you have good luck
B. A way to stay in touch with your friends
C. A way for you to help cybercriminals to spread scams and tricks
D. None of the above

For $2000:
Q: Personality tests are

A. A fun way to learn more about yourself
B. A way for cybercriminals to collect facts about you to collect your private information
C. A way of making you more attractive to the opposite sex
D. None of the above

For $4000:
Q: Pop-Up ads are

A. Funny jokes
B. Just annoying advertisements but generally safe
C. A way to win contests and get fun electronics
D. None of the above

For $8000:
Q: By entering your email address in the "free coupon" pop-up ad after placing an order with Orbitz, Priceline.com, Buy.com, 1-800 Flowers, Continental Airlines, Fandango you get

A. A $10 off coupon on your next order sent to your email
B. A $10 off coupons on your next order sent with your order
C. A repeating charge from a "web loyalty" company on your credit charge
D. None of the above

For $16000:
Q: Everyone knows about the "Nigerian", "work-at-home", foreign lottery, and prescription medicine scams but which of the following is also a scam?

A. Become a laptop tester.
B. Free sports equipment for filling out a survey
C. Bank of America security asking you to change your password
D. All of the above

For $32,000:
Q: Legitimate companies rarely send you emails that require you to enter your account name/username/password immediately or face really bad consequences. How do you check to be sure the email is really from a company you know?

A. Open your web browser and log–on to the site the way you normally would.
B. Click on the link in the email.
C. Nothing
D. None of the above

For $64,000:
Q: If you receive a phishing email you should

A. Report it to antiphishing.com or spam.uce.gov
B. Nothing, it is not going to hurt anyone if nothing is done
C. Reply back to the email with rude words
D. None of the above

For $125,000:
Q: Preventive measures that can be used include

A. Using anti-virus, anti-spyware software and a firewall
B. Thinking twice before opening attachments and clicking links even from people and companies I know
C. Telling everyone who uses a computer about ways to protect themselves and their computer
D. All of the above

For $250,000:
Q: Identity theft only occurs to

A. People with credit cards
B. People who carelessly open attachments
C. People without virus scanning software and firewalls
D. All of the above

For $500,000:

Q: According to http://www.antiphishing.org how many MORE phishing sites did they detect in June 2009 than they did in January 2009?

A. 200
B. 2000
C. 20,000
D. None of the above

For $1 Million!!!:
Q: Sending personal information like a social security or credit card number by email is ok if

A. It is to a well known company
B. It is to my school
C. It is to my family
D. None of the above

Great job!!!
Thank you for playing!