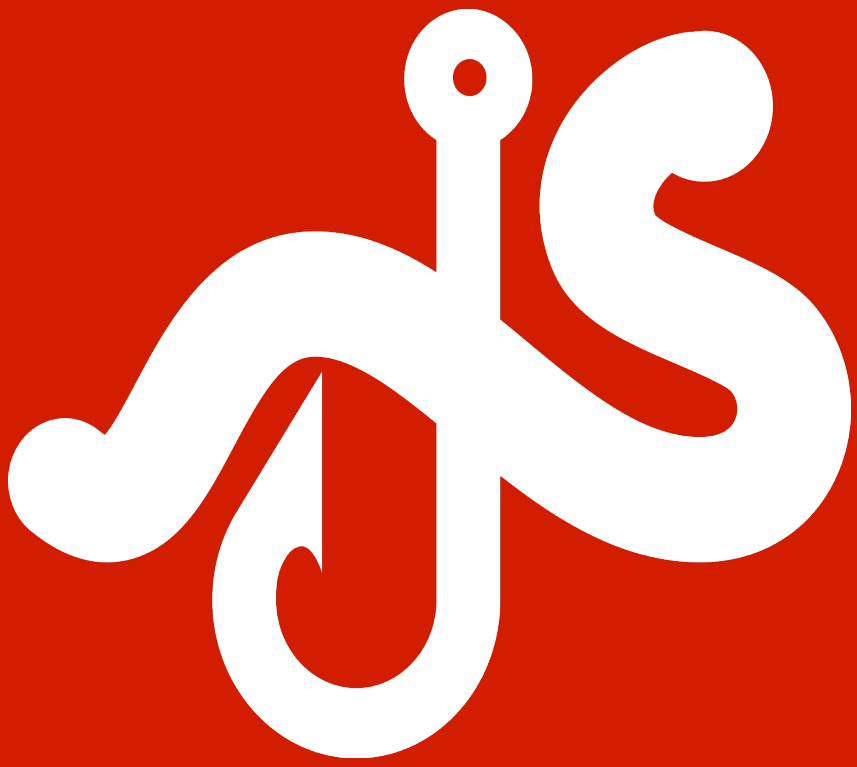
Class 3: Identify Tricks and Scams Online



Google™

iKeepSafe™
PEACE OF MIND FOR FAMILIES ONLINE™

Identify Tricks and Scams Online

Instructor's Overview

DESCRIPTION:

In this lesson, students will learn how to avoid online tricks and scams, and learn best practices of how to conduct themselves online. A student handout booklet accompanies this class.

TIME REQUIRED: Approx. 50 minutes

PREREQUISITES: Students need to have basic computer skills and be familiar with navigating the Internet.

RECOMMENDED GRADE: 6-8

ESSENTIAL QUESTIONS:

How do I protect myself against online tricks?

LEARNING GOALS:

- Students will understand that not everything they see on the web is true, and how to recognize online scams.
- Students will review how to protect themselves from scams.
- Students will know how to take action if they find themselves being scammed.

PREPARATION:

Materials needed:

- Chart paper or chalk/white board
- Student handouts booklet for each student.

Materials recommended:

- Computer with Internet connection and screen projector device for presenter. (Note: if you do not have a screen projector, you can opt to not use the accompanying presentation.)
- Computers with Internet connection for students. (Recommended one per student or one per small group of students, but not required.)
- If you do not have Internet access/computer, be sure to print out the activities in advance.

Optional video:

"Steering Clear of Cyber Tricks": http://www.youtube.com/watch?v=MrG061_Rm7E

VOCABULARY:

Anti-spyware software	protects your computer against security threats and unwanted software
	Chain letter—a letter, email or fax that tells you to send the letter, email or fax to your friends (scams are usually sent out this way)
Firewall	a program that shields your computer from most scams and tricks
Personal information	any piece of information that reveals something about your identity (name, age, address, school, social security number, phone number etc.)
Pop-up contest	often come up as you are browsing the web. They tend to be some sort of game and mention that you have won something. The trick is that they tend to collect information from you
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.
Scam	something that is trying to trick you, often into giving away your personal information

STANDARDS ADDRESSED:

- ALA Standard 8:3: Student will use information technology responsibly.
- 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.
- C3: II:B: Student will make informed decisions about appropriate protection methods and safe practices within a variety of situations.
- C3: II:C: Student will demonstrate and advocate for safe behaviors among peers, family and community.
- 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.
- C3:III:B: Student will make informed decisions about appropriate protection methods and secure practices within a variety of situations.
- C3:III:C: Student will demonstrate commitment to stay current on security issues, software and effective security practices.
- C3:III: D: Student will advocate for secure practices and behaviors among peers, family, and community.
- NETS: 5:a: Student will advocate and practice safe, legal and responsible use of information and technology.
- CCSS: RI.3.5: Use text features and search tools (e.g, key words, sidebars, hyperlinks) to locate information relevant to a given topic efficiently
- CCSS: RI.5.7: Draw on information from multiple print or digital sources, demonstrating the ability to locate an answer to a question quickly or to solve a problem efficiently
- CCSS: W.6.1.b: Support claim(s) with clear reasons and relevant evidence, using credible sources and demonstrating an understanding of the topic or text
- CCSS: 7.1.b, 8.1.b: Support claim(s) with logical reasoning and relevant evidence, using accurate, credible sources and demonstrating an understanding of the topic or text.

Pre-Assessment (3 min)

Start the lesson with some questions to determine the students' knowledge. Teachers may want to divide the students into groups of 4-5 students and have them discuss these questions among themselves. Teachers may also choose for the students to take a survey beforehand. Another option for teachers is to have all students raise their hands and the teacher chooses one person per question.

Ask:

- ***Who uses email in the class?***
- ***Who knows what an online scam is? Give examples.***
- ***Have you ever been scammed via email? Why did you think it was a scam?***
- ***What should you do when you think you are being scammed?***
- ***Who has an account on a social network, including but not limited to, Google+, Facebook, Instagram, Tumblr?***
- ***Is it safe to use your real personal information for an online character? Why?***
- ***How can you get an email scam from someone if you never gave your email address to that person?***
- ***If you get a greeting card from a "secret admirer", should you respond?***
- ***Can scams happen on websites that you visit?***
- ***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?***

Hook or Attention Activity (2 min)

Say: "Imagine you are walking down a crowded street and a complete stranger approaches you and says you have just won a free trip—all you need to give him is your name, age, address, phone number, and passwords to your social network accounts (Google+, Facebook etc). Would you believe him?"

Bridge: "In real life, we wouldn't trust a stranger with our personal information, and being online should be no different. If something sounds too good to be true, it probably is—especially if your personal information is required."

Guidelines to follow (10 min)

Either watch this video by Google, Staying Clear of Cyber Tricks (http://www.youtube.com/watch?v=MrG061_Rm7E)

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."

OR share these key concepts from the video with your class:

How do I recognize cyber tricks, scams, and phishing?

1. Is it giving you something for free? Free offers usually are not free, especially if the offer needs your personal information.
2. Is it asking for your personal information?
    a. 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.
    b. Most legitimate businesses will never ask for personal information like account numbers, passwords and social security numbers via email.
3. Is it a chain letter?
    a. Chain letters may put you at risk.
    b. Don't forward them to your friends.

How do I avoid these tricks?

1. Think before you click. Don't click on any link or file in a suspicious email.
2. 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 bad software.
3. Do a web search for a company's name before you give them any information about yourself.
4. Read the fine print.
    a. At the very bottom of most documents there is what is called the fine print. This text is often barely legible, but many times contains various tricks.
    b. The top of the page may say that you have won a free phone, but in the fine print, it may say that you actually have to pay that company $200 every month.

Oh, no! I got tricked. What do I do?

1. Tell a trusted adult immediately. The longer you wait, the worse it may get.
2. If you are worried about your bank account or credit card information, contact the bank or credit card company immediately.
3. If you received a phishing email, go to www.antiphishing.com to report it!

Hand out "What are Cyber Tricks?" *(Student Handouts p 2)* and go over the tips with the students. If time permits, also discuss "Additional Tips" (*Student Handouts, p 3. NOTE: These tips can also be found at: http://www.google.com/goodtoknow/online-safety/scams/)*

Activity (10 min)

Tell the students that they are about to see some examples of real phishing/scams and online tricks. Teachers can either visit www.sonicwall.com/furl/phishing/index.php and have the students take a Phishing IQ test, or can hand out the phishing scams to the students *(Student Handouts p 4-6)*.

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 extra cautious than be a phish.
- Always think twice before forwarding something, clicking on something or filling out your personal information.

Post-Assessment Activity (30 min)

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.

(Note: these questions include the same pre-assessment questions asked as well as additional questions from the lesson. For teachers who do not have a projector to show the PPT, PDF copies of the questions should be printed in advance and taped to the board)

Divide the class into groups of 4-5 students. Each group can come up with a group name, if so desired. The teacher can either tally the dollars his or herself, or choose a student to do so. The teacher will read the question and then give each group ten seconds to discuss. One student from each group will raise their hand when they have the answer. If they group gets the question right, they earn the points associated with that question.

> Optional ideas: Alternatively, this game can be played in the traditional way where one student is the contestant and the class is the audience. To encourage full classroom participation during the game, you may want to choose to have three lifelines (50-50, Ask a Friend, Ask the Classroom). *50-50* eliminates two of the false answers, *Ask a Friend* allows the participant to ask a friend the question, and *Ask the Classroom* would allow the entire classroom the opportunity to weigh in.

Who Wants to be a Millionaire? A Cyber Security Game

For $100: Is it safe to use your real personal information for an online character?

A. Yes, it doesn't matter.
B. Yes, but only your real name, address, and age,
C. Yes, but only once in a while.
D. **It's better not to reveal personal information, even when creating an online character.**

For $200: 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: Can you get an email scam from someone even if you never gave your email to that person?

A. No, you can only receive an email scam from someone you know.
B. **Yes, phishing scams use software to take other sources.**
C. No, you can only receive an email scam if you give out your email to too many friends.
D. No, only friends and family know your email.

For $500: Which of the following is not a tip to avoid falling for scams?

A. Thinking before you click.
B. Doing a web search for a company's name before you give them any information about yourself.
C. Read the fine print.
D. **All of the above**.

For $1000: 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: 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: 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: 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: 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: 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: 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: 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: Identity theft only occurs to…

A. Adults
B. Youth who share personal information
C. People with firewalls installed on their computers
D. **All of the above**

For $500,000: According to http://docs.apwg.org/reports/apwg_trends_report_Q4_2012.pdf, which industry sector saw a rise in phishing attacks?

A. Social Networking
B. **Gaming**
C. Financial
D. None of the above

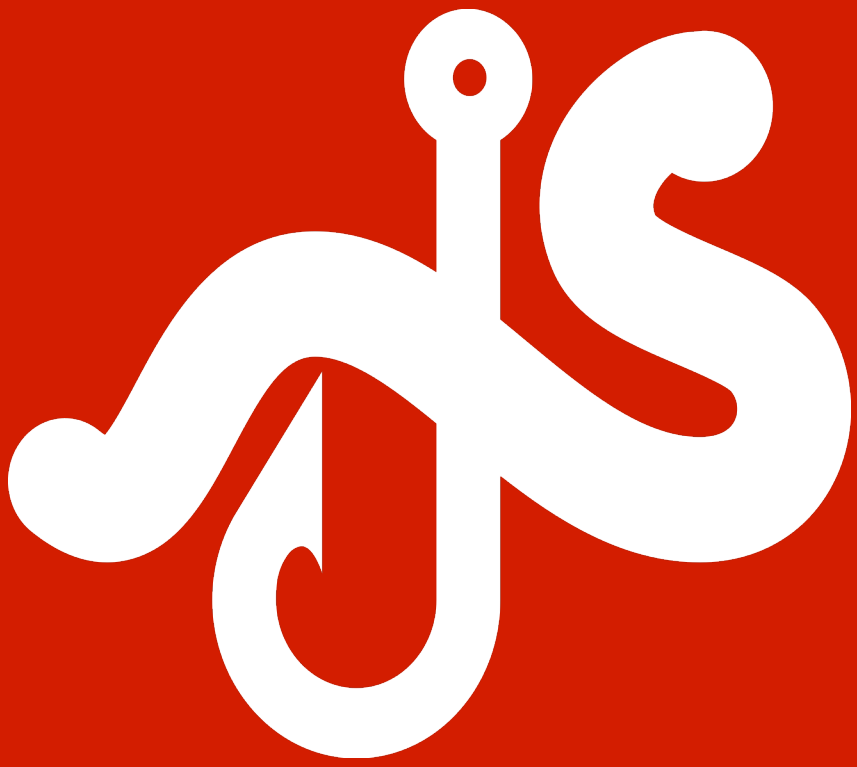
For $1 Million: Sending personal information like a social security or credit card number by email is ok if...

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!

Class 3: Identify Tricks and Scams Online

Student Handout



Google™

iKeepSafe™

PEACE OF MIND FOR FAMILIES ONLINE™

Identify Tricks and Scams Online

What are Cyber Tricks?

How do I recognize cyber tricks, scams, and phishing?

1. Is it giving you something for free? Free offers usually are not free, especially if the offer needs your personal information.
2. Is it asking for your personal information?
    a. 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.
    b. Most legitimate businesses will never ask for personal information like account numbers, passwords and social security numbers via email.
3. Is it a chain letter?
    a. Chain letters may put you at risk.
    b. Don't forward them to your friends.

How do I avoid these tricks?

1. Think before you click. Don't click on any link or file in a suspicious email.
2. 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 bad software.
3. Do a web search for a company's name before you give them any information about yourself.
4. Read the fine print.
    a. At the very bottom of most documents there is what is called the fine print. This text is often barely legible, but many times contains various tricks.
    b. The top of the page may say that you have won a free phone, but in the fine print, it may say that you actually have to pay that company $200 every month.

Oh, no! I got tricked. What do I do?

1. Tell a trusted adult immediately. The longer you wait, the worse it may get.
2. If you are worried about your bank account or credit card information, contact the bank or credit card company immediately.
3. If you received a phishing email, go to www.antiphishing.com to report it!

Additional Tips

No, you probably haven't won the lottery. You can't make that much working from home. And that deal really might be too good to be true. The web can be a great place, but not everyone online has good intentions. Here are three simple ways to avoid scammers and stay safe on the web:

1. Beware of strangers bearing gifts

A message is probably up to no good if it congratulates you for being a website's millionth visitor, offers a tablet computer or other prize in exchange for completing a survey or promotes quick and easy ways to make money or get a job ("get rich quick working from your home in just two hours a day!"). If someone tells you you're a winner and asks you to fill out a form with your personal information don't be tempted to start filling it out. Even if you don't hit the "submit" button, you might still be sending your information to scammers if you start putting your data into their forms.

If you see a message from someone you know that sounds off or strange, it could be that their account may have been compromised by a cyber criminal -– so be careful how you respond. Common tactics include asking you to urgently send them money, claiming to be stranded in another country or saying that their phone has been stolen so that they cannot be called. The message may also tell you to click on a link to see a picture, article or video, which actually leads you to a site that might steal your information – so think before you click!

2. Do your research

When shopping online, research the seller and be wary of suspiciously low prices just like you would if you were buying something at a local store. Scrutinize online deals that seem too good to be true. No one wants to get tricked into buying fake goods. People who promise normally non- discounted expensive products or services for free or at 90% off likely have malicious intent. If you use Gmail, you may see a warning across the top of your screen if you're looking at an email our system says might be a scam – if you see this warning, think twice before responding to that email.

Watch out for scams using the Google brand. Google does not run a lottery. We do not charge training fees for new employees – if you receive an email saying Google has hired you, but you would have to pay a training fee before you can start, it is a scam. Find out more about various scams using the Google brand.

3. When in doubt, play it safe

Do you just have a bad feeling about an ad or an offer? Trust your gut! Only click on ads or buy products from sites that are safe, reviewed, and trusted.

Many online shopping platforms have trusted merchants/sellers programs. These sellers typically have a visible stamp of approval on their profiles. Make sure that the stamp or certificate is legitimate by reviewing the shopping platforms' guidelines. If the platform doesn't offer a similar program, take a look at the number of reviews and the quality of reviews on the seller.

Examples of Cyber Tricks

1) Bank email:

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.

What stands out to you?

2) Gmail Update:

Email Subject: Password change required!

Dear sir,
You need to update your Gmail account information. If this is not completed by December 1, 2014 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.

What stands out to you?

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.

What stands out to you?

4) 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.*

What stands out to you?

5) Lottery scams:
You get an email notifying you that you have just won $650,000!

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.

What stands out to you?

6) Be creative -- write your own cyber trick here: