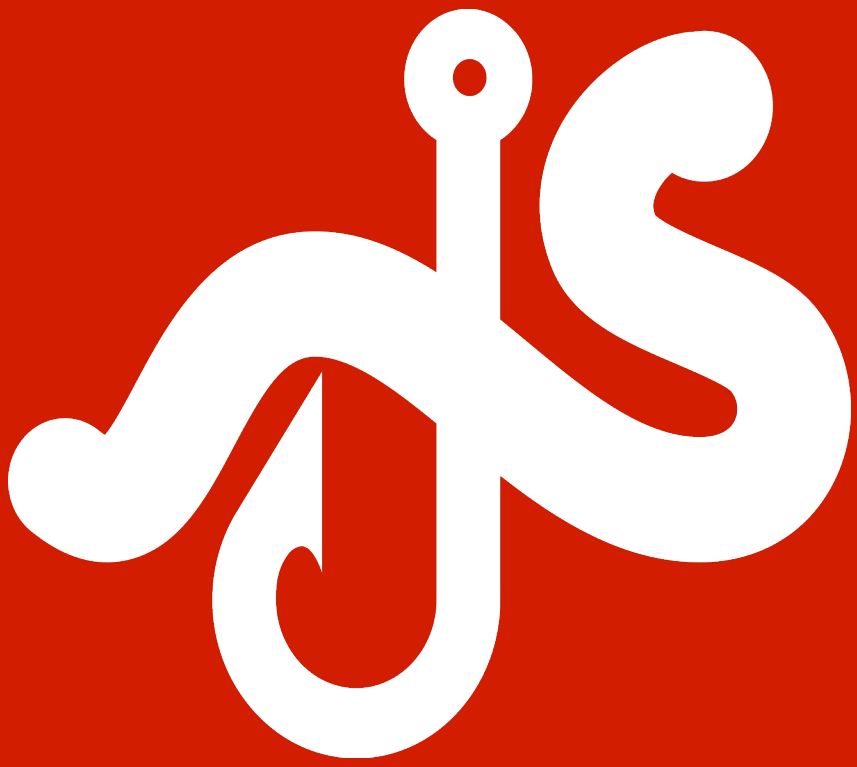
Class 3: Identify Tricks and Scams Online

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: