Workshop 3:
Steering Clear of Cyber Tricks
Student Handouts

Google

iKeepSafe

Table of Contents

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 them to 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.

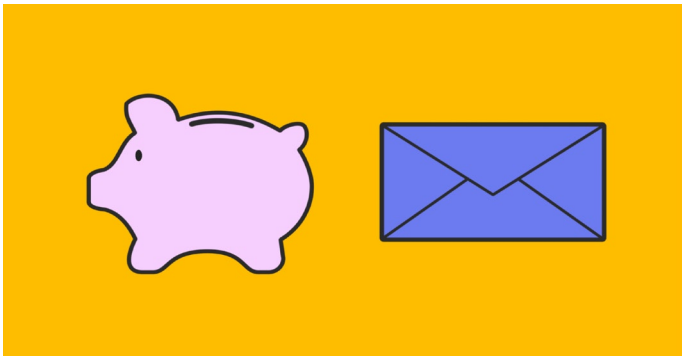
Click here to Change Your Password

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.

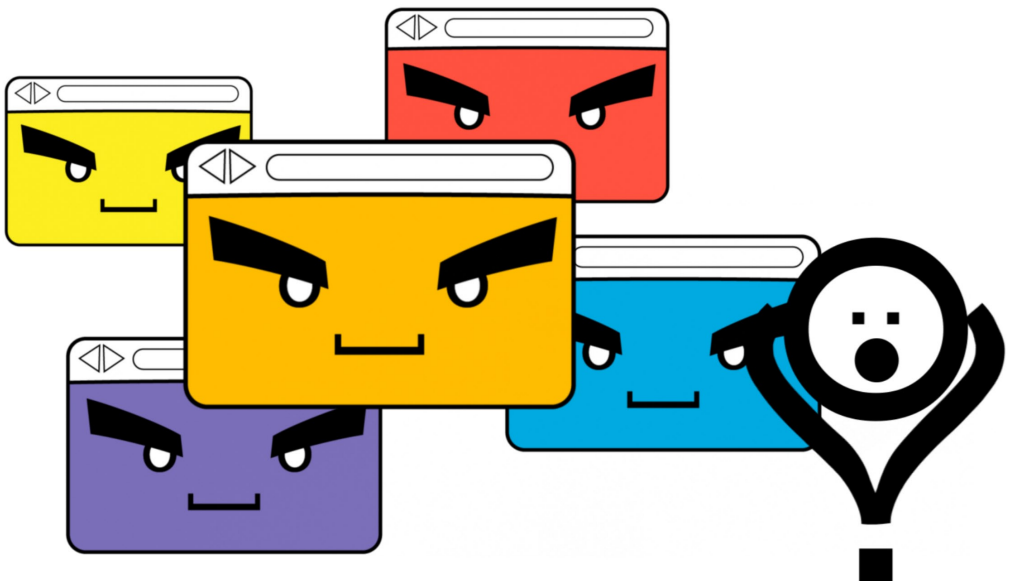


How to avoid falling for the scam:

- ☐ 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.