Intermediate Class, Lesson 3:
Email Safety
Protect me and my new best friend while using emails

Lesson 3 objectives:

In Section A, students will:

- Know what a spoofed email address is.
- Learn what an email attachment is, and how to open it.
- Cautions on opening email attachments.
- Learn why you shouldn’t open every email sent from friends.

In Section B, students will:

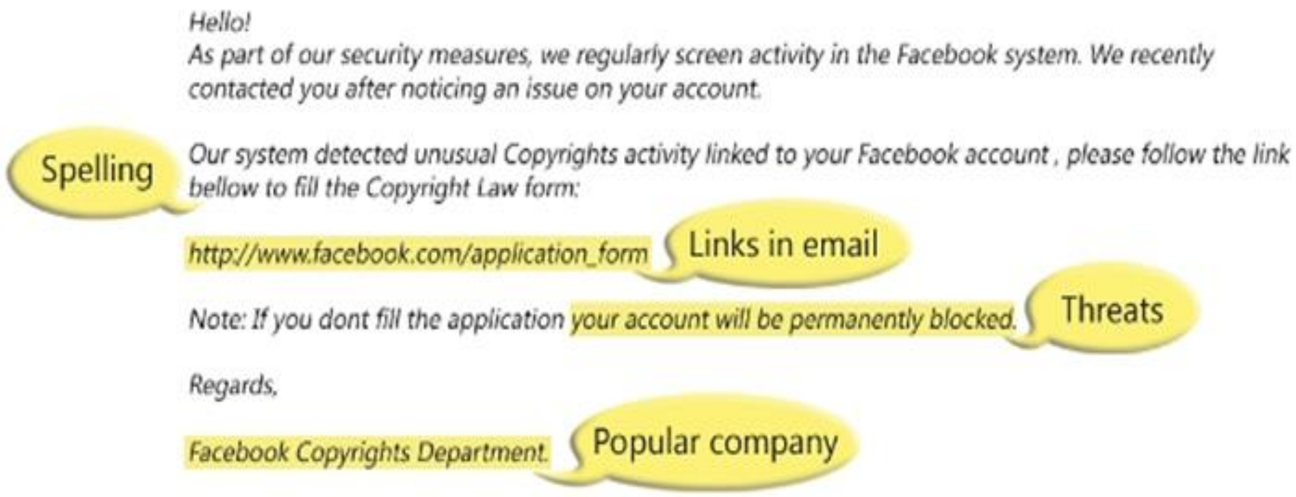
- Practice opening email attachments.
- Practice identifying spoofed emails.
- Practice Identifying unsafe email links.
- Practice identifying false advertisements in junk or spam emails.

BROUGHT TO YOU BY				
BROADBANDUSA CONNECTING AMERICA'S COMMUNITIES	City and County of San Francisco Department of Aging and Adult Services	COMMUNITY LIVING CAMPAIGN	COMMUNITY TECHNOLOGY network	SELF-HELP FOR THE ELDERLY 安老自助處

What is Phishing?

Phishing email messages are designed to steal money. Cybercriminals try to convince you to hand over your personal — and especially financial — information under false pretenses. They often ask you to verify your personal information, such as user name and password to your online banking site, birth date, credit card number, social security number, and checking account numbers. Once they have the information, they can use it or sell it to someone else to steal money from you.

- Here is an example of what a phishing scam in an email message might look like.



Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you dont fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department.

NOTE 1: Spelling and bad grammar. Cybercriminals are not known for their grammar and spelling. A professional company or organization usually has a staff of copy editors that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam.

NOTE 2: Beware of links in email. If you see a link in a suspicious email message, don't click on it. Links might lead you to .exe files. These kinds of files are known to spread malicious software that will harm your computer.

NOTE 3: Threats. Have you ever received a threat that your bank account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cybercriminals often use threats that your security has been compromised.

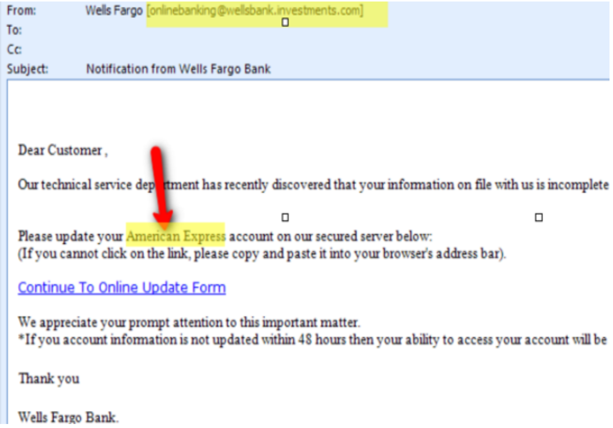
NOTE 4: Spoofing popular websites or companies. Scam artists use graphics in emails that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows. Don't trust an email simply because it looks like it came from a trusted source. Thieves often disguise their emails to look like bank websites or online businesses. They use logos and graphics to look trustworthy.

Here are a few Examples of scam and phishing emails:

You have a bank account with Wells Fargo. An email with the subject line "Notification from Wells Fargo Bank" appears in your Junk Mail folder. It sounds urgent.

Should you open it?

- **Is this a legitimate email?**
- **Why would Wells Fargo ask you to update your American Express account?**



From: Wells Fargo [onlinebanking@wellsbank.investments.com]
To:
Cc:
Subject: Notification from Wells Fargo Bank

Dear Customer ,

Our technical service dep tment has recently discovered that your information on file with us is incomplete

Please update your American Express account on our secured server below:
(If you cannot click on the link, please copy and paste it into your browser's address bar).

Continue To Online Update Form

We appreciate your prompt attention to this important matter.
*If you account information is not updated within 48 hours then your ability to access your account will be

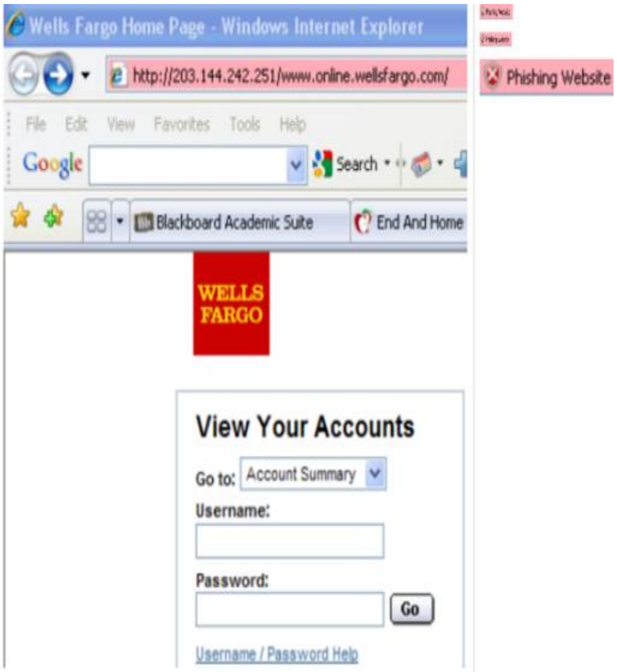
Thank you

Wells Fargo Bank.

Let's say you open the email message and click on the Continue To Online Update Form link. The new page asks you to log into your account by entering your user name and password. Should you enter this information?

- Your web browser often warns you if it believes the website you are visiting is a phishing website.
- The browser will put a notification sign Phishing Website next to the offending website.

You should never give out information in response to emails with questionable email addresses or website addresses.



Wells Fargo Home Page - Windows Internet Explorer

http://203.144.242.251/www.online.wellsfargo.com/

Phishing Website

File Edit View Favorites Tools Help
Google
Search
Blackboard Academic Suite
End And Home
WELLS FARGO

View Your Accounts

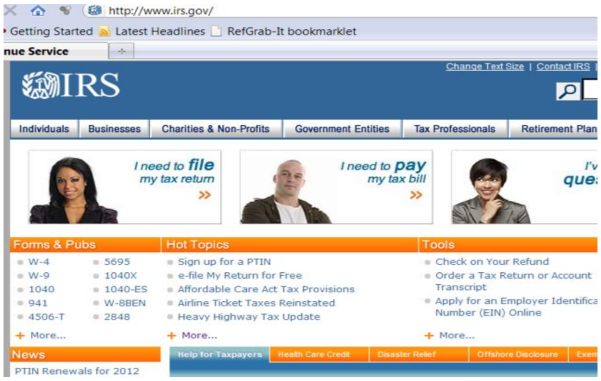
Go to: Account Summary

Username:

Password:

The picture on the right is the real IRS website.

Scammers can make a fake IRS website looks very real, but you should never click on links from such emails because the IRS, banks, and financial institutions will never ask for your personal or financial information over the Internet



http://www.irs.gov/

Forms & Pubs
- W-4
- W-9
- 1040
- 941
- 4506-T
- 5695
- 1040X
- 1040-ES
- W-8BEN
- 2848
- More...

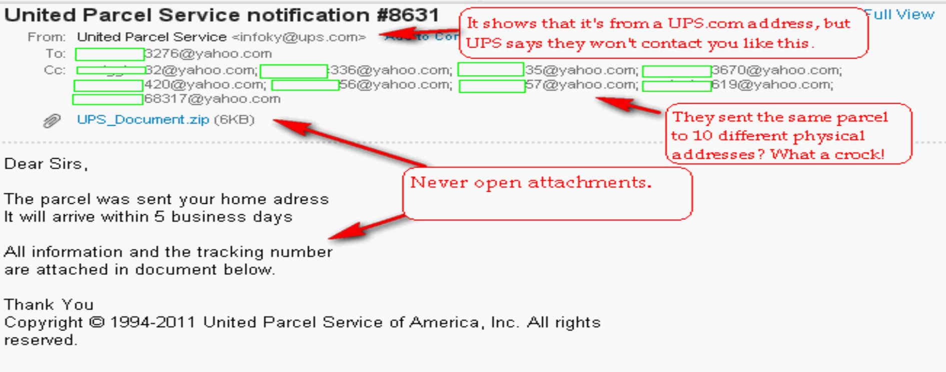
Hot Topics
- Sign up for a PTIN
- e-file My Return for Free
- Affordable Care Act Tax Provisions
- Airline Ticket Taxes Reinstated
- Heavy Highway Tax Update
- More...

Tools
- Check on Your Refund
- Order a Tax Return or Account Transcript
- Apply for an Employer Identifica Number (EIN) Online
- More...

News

PTIN Renewals for 2012

- If you need to go to an important website, type it directly in the address bar!



United Parcel Service notification #8631

From: United Parcel Service <infoky@ups.com>

To: [redacted]3276@yahoo.com

Cc: [redacted]32@yahoo.com; [redacted]336@yahoo.com; [redacted]35@yahoo.com; [redacted]3670@yahoo.com; [redacted]420@yahoo.com; [redacted]56@yahoo.com; [redacted]57@yahoo.com; [redacted]619@yahoo.com; [redacted]68317@yahoo.com

UPS_Document.zip (6KB)

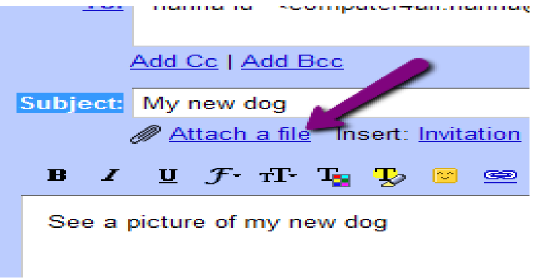
Dear Sirs,

The parcel was sent your home adress
It will arrive within 5 business days

All information and the tracking number
are attached in document below.

Thank You
Copyright © 1994-2011 United Parcel Service of America, Inc. All rights reserved.

Full View
It shows that it's from a UPS.com address, but UPS says they won't contact you like this.
They sent the same parcel to 10 different physical addresses? What a crock!
Never open attachments.

To attach the dog's picture, click on the Attach a file link.	 Add Cc | Add Bcc Subject: My new dog Attach a file Insert: Invitation See a picture of my new dog
1. Select the location of the picture files. 2. Use the **down triangle symbol** in the **Look in:** field to find your USB flash drive location. If your picture files are saved on the desktop, then look in the desktop. 3. Find the file’s name and click on it. 4. Click on **Open** next to the file name and the file will be attached to your email. 5. Use the **Tab** key to move to the **body** field and type in your message. 6. Click on **Send**.	

Questions for next time:

____

____

____

____

____

____