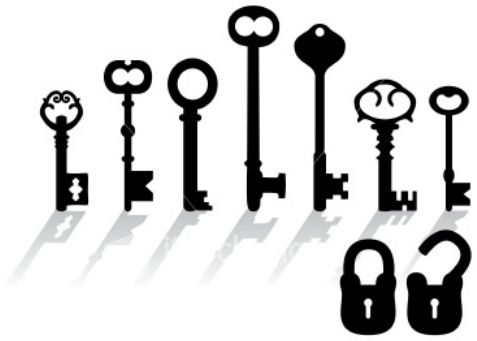
The
New York Society Library
Presents:

Protect Yourself:
Internet Security

Ingrid Richter
Head of Systems

INDEX:

GENERAL TIPS



E-MAIL:

- Don't trust anything sent through e-mail
- Don't open e-mail attachments from unknown senders
- Be cautious of opening attachments from friends and family
- Never send your credit card through e-mail
- Never click on a web link in an e-mail
- Don't respond to anything that requires your immediate attention
- Never give out your password
- Empty your spam folder and trash

WEB:

- Proceed with caution on unfamiliar websites
- Keep an eye open for pop-up ads and don't automatically click anything that pops up.
- Don’t allow websites to install anything on your computer unless you ask first
- Always choose "Custom" or "Advanced Install" for software
- Clean out your cookies/temporary internet history files

VIRUS PREVENTION:

- Back up your computer frequently
- Download and install Critical Updates (Windows users)
- Install & learn to use antivirus software (see page 13 for free antivirus software)
- Keep your virus definitions up to date

PASSWORDS

Campus	Business	Residence
123456	**123456**	**123456**
password	**password**	**password**
12345	**test**	**test**
test	**admin**	**12345**
admin	**test123**	**123**
1234	asutcmhack123@	**1234**
123	*passwd*	**test123**
root	40232046bad	*passwd*
qwerty	!@#asutcmhack!@#	1
abc123	**root**	12
administrator	**12345**	**root**
12345678	**qwerty**	**admin**
user	**1234**	changeme
linux	*mysql*	abc123
test123	**123**	**qwerty**
guest	*apache*	**guest**
mysql	*master*	1q2w3e
1234567	**user**	**user**
apache	*linux*	newpass
master	**guest**	asdfgh

BAD PASSWORDS

- Do not use your e-mail password for anything other than your e-mail account.
- Do not use your bank password for anything other than your bank account
- Do not use your PayPal password for anything other than PayPal.

- Do not use only words for your passwords.
- Use at least seven characters with a mixture of letters and numbers.
- Test your password strength out at: http://www.passwordmeter.com/

Do not use any of these weak passwords from http://lifehacker.com/5505400/how-id-hack-your-weak-passwords

1. password
2. 123 or 1234 or 123456.
3. god
4. letmein
5. money
6. love

7. *Your partner, child, or pet's name, possibly followed by a 0 or 1*
8. *The last 4 digits of your social security number.*
9. *Your city, or college, football team name.*
10. *Date of birth – yours, your partner's or your child's.*

EMAIL: SPAM

Spam is unsolicited e-mail on the Internet. From the sender's point-of-view, it's a form of bulk mail. To the receiver, it usually seems like junk e-mail. It's generally equivalent to unsolicited phone marketing calls.

SPAM EXAMPLE #1:

From: Natalie Sinclair [mailto:novelle9@esfrancisca.com]
Sent: Tuesday, April 27, 2010 10:55 PM
To: Ingrid Richter
Subject: Choose the needed field.

BECAUSE YOU DESERVE IT! Is your lack of a degree holding you back from career advancement? Are you having difficulty finding employment in your field of interest because you don't have the paper to back it up – even though you are qualified? If you are looking for a fast and effective solution, we can help! Call us right now for your customized diploma: Inside U.SA.: 1-718-989-5740 Outside U.S.A.: +1-718-989-5740. Just leave your NAME & TEL. PHONE # (with country-code) on the voicemail and one of our staff members will get back to you promptly!

What the spammer wants you to think:

- Cool! College degree for sale - this will help out in a bad economy! What do I have to lose?

What you should be thinking:

- Even if this is legit, if I respond to this spam, this will put me on a list for future spamming.

What you should do:

- Delete the message, preferably unread. Don't contact the sender for any reason - you don't want the spammers to know that they have a valid e-mail address.

SPAM EXAMPLE #2:

From: Viagra online, genuine formula [mailto:agexe2059@comcastbusiness.net]
Sent: Wednesday, April 28, 2010 8:21 AM
To: Ingrid Richter
Subject: Dear ingrid, Catch 77% discounts hopydoemat

Having trouble viewing this email? View it in your browser <http://mekan.az/tiff31.html>. Drugs for your potency <http://mekan.az/tiff31.html>

What the spammer wants you to think:

- 77% off Viagra?! This is great! Let me just click the link to see the price…

What you should be thinking:

- Why aren't they listing the price? Why do they have 'hopydoemat' in the subject? Why do they want me to visit a website? Is 'cheapest' really 'best' when it comes to medicine?

What you should do:

- Never click on a link in a spam message. Delete the message, preferably unread.

E-MAIL SCAMS

Scams are e-mails asking for money (or offering money). If you send any money, you will be hit up for more money and will never see any of it back.

SCAM EXAMPLE #1:

From: Online Lottery. [mailto:claimsagent@onlinelottery.co.uk]
Sent: Tuesday, April 27, 2010 2:25 PM
To: undisclosed-recipients
Subject: Your Email Was Listed For US4.6m.

UK LOTTERY ORGANIZATION.
ONLINE EMAIL NOTIFICATION.

If you are the correct owner of this email address then be glad this day as the result of the UK lotto online e-mail address draws of 1ST APRILS 2010 has just been released and we are glad to announce to you that your email address won you the sweepstakes in the first category and you are entitled to claim the sum of US$4.6Million. Your email address was entered for the online draw on this Ticket Number: MPP536566301830 and won on this Lucky Number: HJDJ787304JDGD0W.You are to contact Mr.Morse Roland on the below email address for available options on how to receive your winnings fund. Note that Mr.Morse Roland might fail to recognize you as the true winner and receiver of the US$4,600,000 if you fail to include the following in your contact mail to him" Your country of origin and country of Residence/work,complete official names,address,amount won, free ticket and lucky numbers, date of draw,contact telephone and mobile numbers. OPTIONAL :- [Sex,age,occupation and job title].Please do not reply to the sender,instead send your reply to: Contact Mr.Morse Roland.email: uk.morseroland@yahoo.com.hk

CONGRATULATIONS WINNER.

What the scammer wants you to think:

- Hooray! I just won $4.6 million dollars! Look at those ticket and confirmation numbers!

What you should be thinking:

- I never entered a lottery. Why would they give away free money? Why are there so many typos and grammar mistakes? Why do I have to contact someone in Hong Kong for a UK lottery? Why are they paying the amount in US$?

What is really happening:

- The scammer wants your valid contact information to trick you out of 'fees' and 'services' for transferring this fake money. Sometimes they'll even ask for your bank account information. You will never see the money - the lottery is obviously fake.

What you should do:

- Don't contact the sender and don't sent any personal information through. Delete the e-mail and chuckle over the imaginary $4.6 million dollars that you 'won' from having a valid e-mail address.

E-MAIL SCAMS (CONT):

From: Robert Haworth <rfhaworith@hotmail.com.xxx>
Subject: I NEED YOUR HELP URGENTLY AND PRAYER
To:
Date: Tuesday, February 9, 2010, 3:33 AM

How are you doing today? I am sorry i didn't inform you about my traveling to ENGLAND for a EVANGELISM program which is taking place in ENGLAND . It as been a very sad and bad moment for me, the present condition that i found myself is very hard for me to explain.

I am really stranded in ENGLAND because I forgot my little bag in the Taxi where my money, passport, documents and other valuable things were kept on my way to the Hotel am staying, I am facing a hard time here because i have no money on me. I am now owning a hotel bill of $1500 and they wanted me to pay the bill soon else they will have to seize my bag and hand me over to the Hotel Management, I need this help from you urgently to help me back home, I need you to help me with the hotel bill and i will also need $2000 to feed and help myself back home so please can you help me with a sum of $3500 to sort out my problems here? I need this help so much and on time because i am in a terrible and tight situation here, I don't even have money to feed myself for a day which means i had been starving so please understand how urgent i need your help.i have decided not tell my family so that they will not be worried.when I return I will tell them and they will understand.

I am sending you this e-mail from the city Library and I only have 30 min, I will appreciate what so ever you can afford to send me for now and I promise to pay back your money as soon as i return home so please let me know on time so that i can forward you the details you need to transfer the money through Money Gram or Western Union.Hope to hear from you.

Regards.

Robert Haworth

What the scammer wants you to think:

- I know Bob Haworth, and he is a minister. He must be in serious financial trouble to be e-mailing me. This sounds urgent and bad. Poor guy!

What you should be thinking:

- Hmm, haven't heard from Bob in ages, and $3,500 is a lot of money. How did he check into a hotel if he didn't have credit cards? Does anyone need $2,000 to feed themselves? Why did he spell his name wrong in his e-mail address? Why is his grammar and spelling so awful? Why is there nobody in the To: field of this e-mail?

What is really happening:

- Someone spoofed Bob Haworth's e-mail address and sent out a targeted plea pretending to be him. They're probably not expecting the full $3,500, but any money you send is free money for them.

What you should do:

- Don't send any e-mail to the sender (Money Gram and Western Union will never refund your money). If you want, find the original person's e-mail or phone number and let them know that someone is doing this on their behalf, so that other people don't get scammed.

E-MAIL HOAXES

Internet hoaxes and chain letters are e-mail messages written with one purpose; to be sent to everyone you know. The sender is known to the user, the threat sounds realistic, and the urgent nature prompts immediate action.

HOAX EXAMPLE: The "Guts to Say Jesus" Hoax

Subject: New Virus Alert

Very Urgent!!!!!!!...
PASS THIS ON TO ANYONE YOU HAVE AN E-MAIL ADDRESS FOR.

If you receive an email titled: "It Takes Guts to Say Jesus" DO NOT OPEN IT. It will erase everything on your hard drive. This information was announced yesterday morning from IBM; AOL states that this is a very dangerous virus, much worse than "Melissa," and that there is NO Remedy for it at this time. Some very sick individual has succeeded in using the reformat function from Norton Utilities causing it to completely erase all documents on the hard drive. It has been designed to work with Netscape Navigator and Microsoft Internet Explorer. It destroys Macintosh and IBM compatible computers.

This is a new, very malicious virus and not many people know about it. Pass this warning along to EVERYONE in your address book ! and please share it with all your online friends ASAP so that this threat maybe stopped. Please practice cautionary measures and tell anyone that may have access to your computer. Forward this warning to everyone that you know that might access the Internet.

Joyce L. Bober IBM Information Systems
Pittsburgh Mailing Systems 412 - 922-8744

What the hoax sender wants you to think:

- I'll be doing a great public service to all my friends and family by forwarding on this message! This might prevent more computers from getting infected!

What you should be thinking:

- Why haven't I heard of this virus in the news? Why is my non-tech-savvy friend sending me this? Why am I required to do all this social work for a new virus threat?

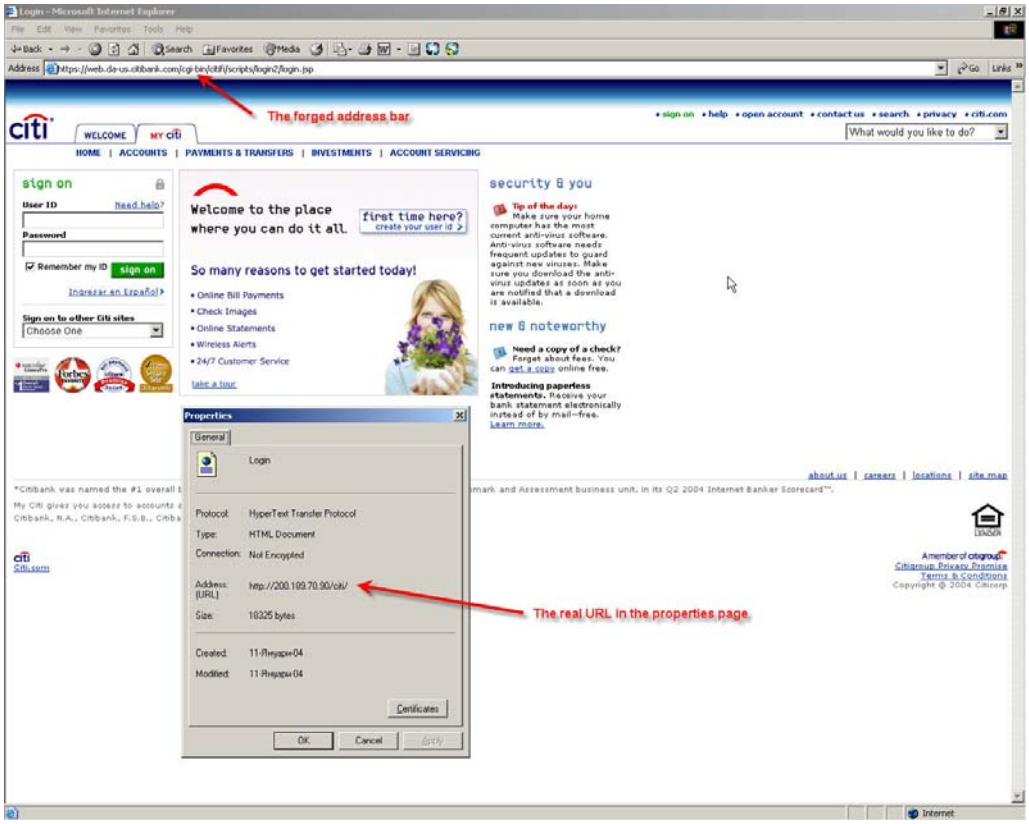
What you should do:

- Don't send this e-mail out to anyone - you'll just look foolish. Research it online by finding the unique elements in this e-mail ("It Takes Guts to Say Jesus") and search Google for it. Send a gentle e-mail back to your friend, informing him or her that this is a hoax and isn't real.

WEB PHISHING

Phishing sites use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. Never click on a link in your e-mail to verify information. Be highly skeptical of e-mail notification of account closures or money owed, especially from banks, eBay or PayPal.

PHISHING EXAMPLE: A Citibank Phishing Site



<u>What the phishing site wants you to think:</u>

- This looks exactly like my Citibank page! Let me enter my login and password…

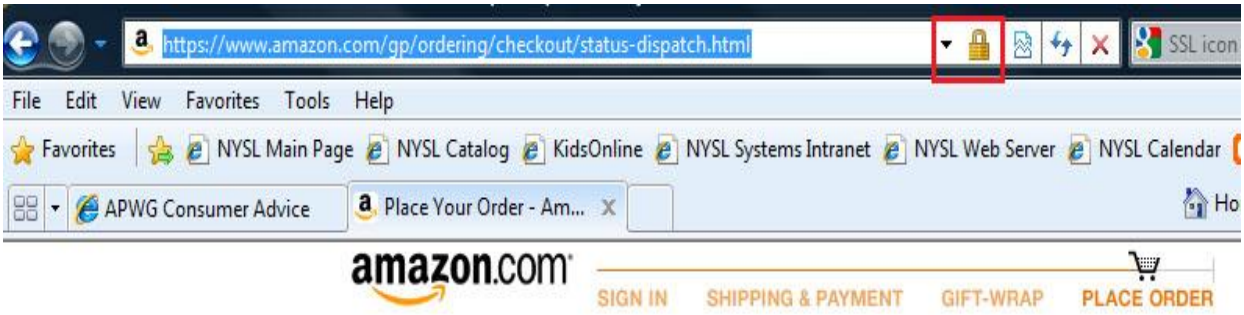
<u>What you should be thinking</u>:

- Why is the bank instigating new measures online? Why do they want me to log in to change a setting? Why do things look a little funny in the address bar at the top of the screen?

<u>What you should do</u>:

- Never click on a link in an e-mail. Report any fake website to your bank or financial information - they have as much reason to be upset about this as you do and they have the power to go after the people responsible for creating the fraudulent site.

SECURE ORDERING



TIPS FROM ANTIPHISHING.ORG

http://www.antiphishing.org/consumer_recs.html

Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser (see lock icon in the box next to the web address).

The lock box location and icon will differ from browser to browser (and operating system), so become familiar with your version and where this lock box appears. This lock should appear on airline sites, Amazon.com and any page where you might be prompted to enter a credit card number. If you do not see the lock box on a site while ordering, do not enter your credit card number on the page (call in your order or fax the credit card number to them instead).

Double-click on this for more information about the security certificate of the website. You cannot force this box to come up - this is done through the other website.

Keep in mind:

- Phishers are now able to 'spoof,' or forge BOTH the "https://" that you normally see when you're on a secure Web server AND a legitimate-looking address. You may even see both in the link of a scam email. Again, make it a habit to enter the address of any banking, shopping, auction, or financial transaction website yourself and not depend on displayed links.

- Phishers may also forge the yellow lock you would normally see near the bottom of your screen on a secure site. The lock has usually been considered as another indicator that you are on a 'safe' site. The lock, when double-clicked, displays the security certificate for the site. If you get any warnings displayed that the address of the site you have displayed does NOT match the certificate, do not continue.

Remember not all scam sites will try to show the "https://" and/or the security lock. Get in the habit of looking at the address line, too. Were you directed to PayPal? Does the address line display something different like "http://www.gotyouscammed.com/paypal/login.htm?" Be aware of where you are going.

SPYWARE

http://www.safer-networking.org

Spyware is a program installed on your computer that keeps track of your web surfing and sends the information back to the owner. It isn't illegal, but it will send targeted pop-up ads to your screen and will slow down your Internet connection.

SPYWARE EXAMPLE: Spyware Protect 2009

What the spyware wants you to think:

- I've been infected by a virus and am under attack! I definitely want to protect myself from this attack. Let me press "Yes"!

What you should be thinking:

- This doesn't look like my virus software -it's not even the same colors. Why do they ask if I want to block an attack - shouldn't it be obvious that I do?

What you should do:

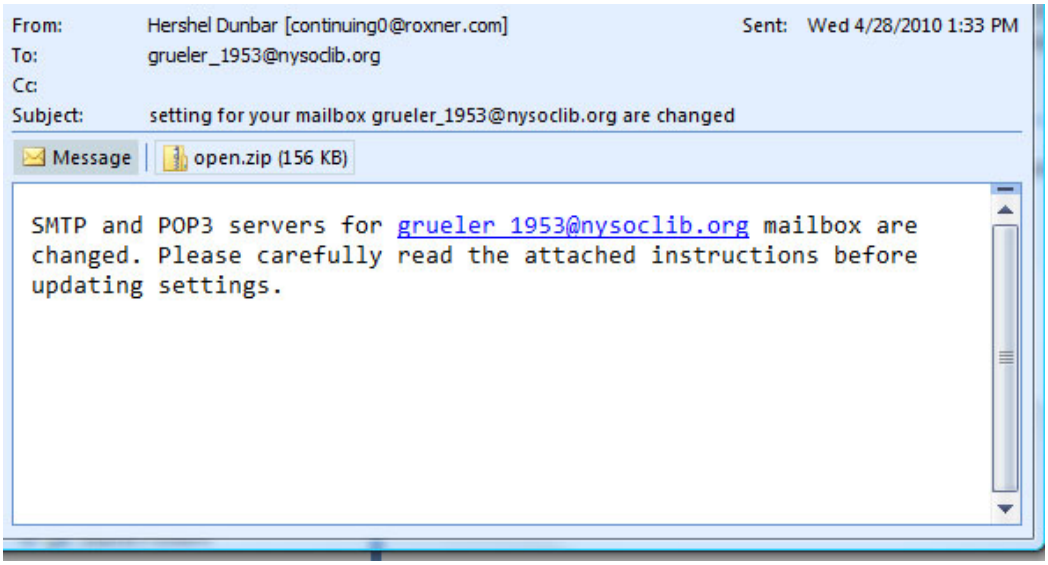
- Right now, you're probably already infected with spyware. Do not click "Yes", but be careful about clicking "No" or trying to close the window. The best course of action would be to force close your web browser by right-clicking on it on the taskbar and choosing "Close". Alternately, you could try holding down CTRL+ALT+DEL and choosing Task Manager to kill this window. This *might* prevent you from being infected.

  Run a virus scan as soon as possible and be on high alert for any other pop-up messages. Write down the unique name ("Spyware Protect 2009") and do a Google search on it in quotes as soon as possible to see how to remove it from your computer.

VIRUSES

To prevent viruses from infecting your computer, never open suspicious e-mail messages, back up your information regularly, download Critical Updates from Microsoft if you are on a PC (http://windowsupdates.microsoft.com), install an anti-virus program and keep the definitions up to date.

VIRUS EXAMPLE: Unknown Virus



What the virus wants you to think:

- This sounds official and boring, but I'd better make the changes. Let me just open the attachment open.zip

What you should be thinking:

- Shouldn't my company/IT department be doing this? Why are they asking me to change the settings? Why did they send this to a fake e-mail address: grueler_1953? Why didn't they include the instructions in the e-mail instead of sending them as an attachment?

What you should do:

- Close this e-mail carefully, delete it from your e-mail and empty your trash bin as soon as possible. Assume the highest level of security while dealing with this message. Absolutely do not click on the attachment - your computer will be infected if you do.

- Never open an attachment from your mailbox unless you are expecting an attachment. Ideally, never open this e-mail in the first place and delete it sight unseen. If you never read the e-mail and never touch the attachment, your computer won't be infected with this unknown virus.

VIRUS REMOVAL

The easiest way to tell that your computer has a virus is by running a complete system scan with updated virus definitions. The tools listed below are all free to download or scan online; anti-virus companies make their money from subscriptions - not from removing viruses on your computer.

Beware of icons popping up on your desktop with strange names and extensions. It's not always a sign that your computer is infected, but it's a good idea to start scanning your hard drive. If your Internet connection is extremely slow and sluggish, and your computer is working overtime to perform even simple tasks, you might also have a virus.

FREE VIRUS REMOVAL TOOLS:

Stinger from McAfee
http://vil.nai.com/vil/stinger/

Housecall from TrendMicro:
http://housecall.trendmicro.com/

FREE ANTIVIRUS SOFTWARE:

AVG Anti-Virus Free Edition:
http://free.avg.com

Avast AntiVirus Software:
http://www.avast.com/free-antivirus-download

NOTES:

These notes are available as a PDF on the New York Society Library website at:
http://www.nysoclib.org/tech/internet18.html

New York Society Library

Internet Security

Friday, May 14, 2010 at 10:00 AM

NAME
(optional):_____

1. Was this workshop worthwhile?

2. Do you feel more comfortable with Internet Security?

3. Was the printed handout useful?

4. What would you like to have seen covered more? Less?

5. Would you be interested in additional workshops?

6. Any other comments? (please use back of paper)