Internet Safety and Security

Overview

- This class will focus on security in online transactions, including email, online ordering, and banking.
- We will also discuss using public computers such as the ones found in the library as well as those you use at home.

General Internet Safety on Public Terminals (i.e. the library)

- Try to avoid conducting financial business online on a public terminal. Someone may walk behind you and see sensitive financial information. It is also possible that a hacker could access your information from your station after you leave. If you must do this at the library, check out a laptop (available at the reference desk) and use a private study room.
- Make sure you close all open windows after you are done using the computer. This will remove cookies and temporary files that could be revealing to anyone sitting down when you finish.
- Make sure you do not save any email or other account passwords on public computers.

General Internet Safety at Home

- Consider using a browser other than Internet Explorer. Because most people use IE, most hackers focus their attention on writing viruses and hacks for it. Try Firefox (www.mozilla.com) or Safari (www.apple.com/safari/download/) instead.
- Install patches as soon as they are released. Patches for Microsoft can be found on windowsupdate.microsoft.com. Apple patches are located on www.apple.com/support/downloads/.
- Pay attention to signs of a virus: significantly slower speed, redundant files, a new homepage that you didn't select, popups that address you by name, etc. Run a virus scan frequently. Some well known ones are Norton (www.symantec.com) or McAfee (www.mcafee.com).
- Avoid file sharing. If you do file share, take files from other people. Do not share your own.
- Don't click on popups. Many will direct you to websites that automatically download spyware and malware.
- Try to avoid downloading unnecessary programs. Some examples include Weatherbug and Smileycentral downloads. Many of these types of programs are actually spyware.
- If your computer is shared, delete your browsing history and cookies. This can be done under the "tools" tab in your browser.
- Use a firewall.
- Secure your wireless connection with a good password. Unsecured connections can be used by anyone. At the very least, this will mean your connection is very slow. In a worst case scenario, someone may use your unsecured connection to gain access to your personal information.

Email

- For many people this is the only part of the internet that they use. Email is an incredibly useful tool when used safely.
- First, pick a strong email password. This means it should have uppercase and lowercase letters as well as numbers. Change this periodically. Remember to log out when you are finished.
- Make sure you uncheck the box that asks you if you would like your password saved.
- If you get a lot of junk email, consider setting up a second email account with a free service such as Yahoo (www.yahoo.com) or GMail (www.gmail.com). This way, you'll have an email for friends and family, and a second for normal internet use (for example, if a website asks you to register with your email.) This only takes a few minutes and can save you lots of time from day to day.
- Take a few minutes to set up your spam/bulk email filter. Make sure you check this folder periodically to ensure that important emails don't end up there.
- Do not click on any links within an email. Often times there is an underlying "hidden" link that will take you to a false website. If you are interested in the website, type the address into your browser.
- If you receive junk mail, do not click "unsubscribe." This will not actually unsubscribe you from the emails and will just verify that the email address you are using is valid.
- Watch for misspellings and errors in punctuation. These can indicate that the email you've received is a scam.
- Try to avoid the many advertisements for survey takers. While people do sometimes make money taking surveys for companies, it is more likely that your email address will be sold.
- When sending email, remember that your message goes through several servers to get to the message recipient. If you would not walk up to someone on the street and give them the information that you are emailing, don't send it.
- Avoid forwarding mail. If you must, delete everything that isn't pertinent.
- Some scammers will try to convince you to do things like email your credit card number to pay for a purchase. Don't fall for this.
- Use your head. If something seems too good to be true, it is. Here are some things to look for:
- Phishing. Phishing is a form of email fraud where a message is sent out to thousands of people at once to try and obtain personal information. The emails look like they are from reputable institutions like banks, businesses, or online sellers like Ebay. In reality, they are from criminals trying to obtain sensitive personal and financial information. When you click on links from the emails, you are directed to websites that look real. You are asked to provide account numbers and other information. Often, victims of phishing have no idea that they've been scammed until charges start showing up on their bank statements.
- To combat phishing, immediately delete any email from governmental agencies, online stores, or financial institutions that ask you for personal information. Reputable organizations will never contact you in this way.

- If the email looks like it is from your bank: forward it to the bank (the email addresses are listed on the websites). Then log into your online bank account and check the message center. If the bank has any legitimate business with you, it will be conducted there.
- If it appears to be from Ebay: check in the message center. If the email is reputable, there will be a copy of it in your secure site. Find more information on how to be safe on Ebay at http://pages.ebay.com/securitycenter/index.html?_trksid=m40.
- Don't be taken in by emotional pleas for help via email. For example, many people received emails asking for donations after the 9/11 attacks and after the tsunami in 2004. Instead of going to reputable agencies that could use the money to help victims, the cash went to criminals. Other versions of this scam include pleas for help for children with cancer, etc. If you would like to give money to a particular cause, go directly to the organizations website.
- Don't fall for the "Nigerian scam." This is one of the oldest and most profitable scams around. A person receives an email requesting help moving cash from another country to the United States. Generally the email is purportedly from a widow or a child who has come into a large amount of cash and needs help getting it out of the country, usually because of an unstable government. For allowing the person to put the money in your bank account, you are offered a large percentage to keep. The scam can make money in several ways. You may give them your bank account number so that they can deposit the money. The criminals will clean out your bank account and you'll never hear from them again. Or, they'll send you a check to deposit. Typically they will ask you to withdraw a portion of the cash right away to send to them for some emergency. By the time you receive word that the check has bounced, the criminals are nowhere to be found and you're left with the overdraft. Another way that this can work is that you are asked for "small" amounts of money, a few thousand here and there, to pay transfer fees, official bribes, etc. The scammers take you for all the money in your bank account and then disappear. These scams are wildly profitable for criminals. In 1997, one Secret Services agent estimated that in the United States alone over $100 million dollars had been reported scammed in the previous 15 months.
- To avoid being the victim of one of these scams, avoid opening emails from anyone you don't know. Especially avoid opening any attachments that you were not expecting.
- www.snopes.com has lots of information about hoaxes and how they work.

Online Ordering

- Buying online is fast, convenient, and generally safe. By taking a few simple steps, you can shop online in relative safety.
- Try to use vendors that are well known, for example, Amazon, Borders, Gap, etc. It is in these stores best interest to provide advanced protection for their buyers. Because they are high profile, they want to avoid any consumer concern about security that might result in a loss of sales. Make sure that the company has a

physical address, phone number, or fax so that you can contact them if there are problems with your order.

- If you are unfamiliar with the vendor, read their security policy (this is usually found at the bottom of their main page.) You can also Google the company to find reviews on their service and security. A few negative reviews are normal, but beware of many. Also check the website of the Better Business Bureau (www.bbb.org) to find out if the business has any complaints against them. The BBB will detail what the problem was and if it was able to be resolved satisfactorily.
- Look for a secure browser once you reach the "checkout" part of your transaction. There should be an "https://" in the address bar of the website as well as a padlock at the end of the address bar. Click on this padlock to get information about the security certificate of the website. This helps you determine if the company has put measures into place to protect your information from hackers. These measures are called "encryption." The process scrambles your information when your computer sends it over the internet. When the business receives the information, it is reassembled and used to complete the transaction. Encryption is not entirely hacker or tamper-proof, but it does make it extremely difficult to get information. Hackers tend to gravitate toward easier targets, so using websites with better encryption and security certificates will greatly reduce any likelihood of your information being viewed.
- Many vendors ask if you would like to receive related email offers from partner companies. Uncheck this option to reduce the amount of spam you receive.
- Some online stores will ask you if you would like your password saved. Do not choose this option.
- After you've ordered your items, you will receive one or more confirmations from the company. Generally there is one to inform you that your order has been received and another when it has shipped. Print these and keep them for your records.
- After you've received your items, you may want to consider deleting the confirmations from your email.

Online Banking

- Each year, millions of Americans avoid banking online for fear that their identity will be stolen or their security compromised. In reality, a 2005 Javelin Identity Fraud Survey Report found that only 11.6% of identity theft occurred because of activities online. The majority of these crimes are still committed traditionally, by digging through trash or stealing wallets. Victims of the theft who monitored their bank accounts online also lost about 1/8 of the amount of money as those who noticed problems on a paper statement.
- There are many benefits to banking online. Because you can choose to stop paper statements for electronic ones, there is less of a chance that someone might steal your account numbers. It is easier and faster to detect fraud. It is also possible to notice any billing or charging issue faster. By banking online, you are taking advantage of the significant security physical and electronic security offered by

your bank. To find out more about the security in place for your protection, visit the website for the bank.

- There are several ways to be safe when banking online.
- Your bank will never ask for your information via email. Do not share usernames, passwords, social security numbers, or any other personal information in email. Most banks have a message center that is located on the main page of your account. If you need to contact your bank, call or use this mail system. It is protected by the highest security possible.
- Also, do not ever click on a link in an email, even if it looks like the email is from your institution. The true URL in the link is easily disguised. Instead, type the address of your bank into your browser and conduct your business from there.
- Banks will not allow you to save both your username and password. However, some will let you save the username. Do not do this, as this makes it much easier for a thief to access your accounts.
- Pick a strong password. Change this password periodically, especially if you suspect that your information has been somehow compromised.
- Always log out when you have finished your banking session.
- Avoid banking (or other financial transactions) on public terminals. A savvy hacker may sit down at the station after you and recall your information.
- Explore the bank website. Most will have a significant section devoted to security-both theirs and yours. For example, Chase has dedicated a large portion of their website to information security (www.chase.com, on the left side of the page).
- Check your credit regularly. This will help you quickly spot any unusual financial activity. The three major credit bureaus are Experian (www.experian.com), Equifax (www.equifax.com), and TransUnion (www.transunion.com). Check your reports free at www.annualcreditreport.com.
- If you notice anything suspicious call your bank immediately.

Finally…

- If you see something unfamiliar, do your best to learn about it. You can google it, or call the library and ask for more information.
- Be cautious, but not afraid. The internet can seem daunting, but it is a wonderful tool. If you use common sense, you should be able to have a great online experience.
- If you have questions, feel free to call the Reference staff at the Barrington Area Library at 847-382-1300. You can also reach us at adultref@barringtonarealibrary.org.