Protecting Yourself on the Internet

Presented by Gini Pedersen to Osher members -- October 29, 2013
http://www.iteachyou.com

1. Security Software

A. Need protection for **all** of the following security threats:
(1) Viruses
(2) Firewall Hackers
(3) Spyware/Scamware/Scumware

B. Security Suites (All-in-One Protection)
(1) **If using Windows 7, Vista, or XP**: You can choose to download a free suite called Security Essentials from Microsoft. Go to http://www.iteachyou.com/essentials.htm for details.
If using Windows 8: You already have Windows Defender installed and running in the background.
(2) Trend Micro Internet Security --http://www.trendmicro.com
If using a Macintosh -- http://www.intego.com
(3) Norton Internet Security -- http://www.symantec.com
If using a Macintosh -- Norton Internet Security for a Mac
(4) BitDefender Internet Security -- http://www.bitdefender.com
Not currently available for a Mac
(5) McAfee Internet Security -- http:.//www.mcafee.com
If using a Macintosh -- need to buy individual security pieces

C. Issues to consider:
(1) Free or fee?
(2) Buy online or at a store?
(3) Renew online or buy new version?
(4) Single vs. multi user version?

Whichever security software option you select, be sure to confirm the following:

- That your security solution includes protection against viruses, hackers, and spyware.
- It updates automatically for a specified period of time.
- It is actively running in the background during every computing session.
- It supports your version of your Windows or OS-X.

Security software for a handheld PDA (Personal Digital Assistant) or SmartPhone such as an iPhone, Android, Samsung Galaxy, Blackberry, etc. is **not widely available yet**. Therefore, even though you may not be **storing** any personal or sensitive information on a one of these devices that connects to the Internet wirelessly this information can **possibly** be "visible" to hackers while you are actually typing/sending the information. Therefore, it is best to **not** transmit any sensitive data (banking, purchasing, etc.) on one of these devices.

2. Phishing/Scams

A. Definition

Email messages pretending to be another person/company trying to entice you to do something. It is usually sent out to numerous email addresses at a time, counting on some recipients falling for the scheme.
For example: give personal info, buy something, react to a message, etc.

B. Guidelines to follow:

1. **No reputable company or organization will send you an email that requires you to click on a hyperlink to respond. They may include a hyperlink but also suggest you log on to your account at their website if there's something they want to let you know.**
2. If you "hover" over a hyperlink in the email message and the web address listed in the Status Bar at the bottom left of your screen is different than the address in the email message, it's very likely that this email is phishing.
3. If you receive an email that you believe is phishing, DO NOT RESPOND TO IT. Instead, go to the website related to your account, log on, and see if this company has been trying to contact you.

3. Passwords

A. Options

(1) Risky: Online password managers - select one of these **carefully**
eg: http://www.passwordsafe.com or http://www.passpack.com or http://www.lastpass.com

(2) Risky: Program for managing passwords - select one of these **carefully**
egs:
(a) LastPass
(b) Dashlane
(c) Roboform
(d) Password Box
(e) Keeper
(f) MyLok
(g) Kaspersky Password Manager
(h) Password Genie

(3) Risky: Printed list (stored only on password-protected flash disk)

(4) Slightly risky: Fingerprint Reader or Retina Scanner

(5) Not risky: Memorize all ☺

B. Notes

(1) Use strong passwords -- combo of alpha/numeric and upper/lowercase
Examples:
(a) BAD: 11911 (your address, 11911)
(b) BETTER: 11911wf (if registering at Wells Fargo)
(c) BEST: 1W1E9L1L1S -- or maybe WeLLs11911FaRgo

(d) BAD: ILOVETOPLAYTENNIS
(e) BETTER: ilOveTOplAyTeNnIs
(f) BEST: IL2pTVm (stands for I love to play tennis very much)
or il2ptvmwf (if, for example, the password is for Wells Fargo)

(2) Leave a copy in safe deposit box, with attorney, or with trusted person

(3) Change a password immediately if you think it has been compromised.

(4) More information: http://www.iteachyou.com/password.htm

4. Wireless Connections on your Computer

A. **In your house: You have more control**

(1) Your router allows signal to be picked up by all computers within range -- usually less than 100 feet

(2) Difficulty reaching vertically -- upstairs/downstairs

(3) You can't adjust sensitivity; can add a range extender or wireless repeater

(4) To test connectivity distance, take a laptop outside and watch the relative signal strength of your network as you walk further away from the router.

B. **On the road: You have less control** (eg: Starbucks, library, airport, hotel, cybercafe, friend's house)

(1) Allows you to connect your laptop to their wireless connection with radio waves (if available)

(2) You are using a wireless connection other than your own and have no control over how secure it is.

(3) You are vulnerable to intrusions from other computers in the area (library, airport, etc.)

(4) **If using your own computer away from home**...
(a) Be sure your security software is adequate and up to date.
(b) Be sure that no one is watching your keystrokes as you type.
(c) Be sure that security updates are installed for your Operating System.
(d) Best to **not** transmit any sensitive data (banking, online purchasing, etc.).

(5) **If using a public or someone else's computer**, you have no control over installed software or other security settings. Therefore, avoid doing online banking or even other Internet activities that require a password on a public or borrowed computer.

5. Security Updates for your Operating System

A. Automate -- I recommend you set your operating system to automatically download and install security updates for your operating system:

(1) Windows 8: At Win8 Start screen type Control Panel (which automatically opens Search utility) and click to open Control Panel on left side of screen. Click System and Security **only if available** - Windows Update - Change Settings).

(2) Windows 7: Start - Control Panel; Click System and Security **(only if available).** Click Windows Update - Change Settings (or Start-Control Panel-System and Security-Win Update-Change Settings).

(3) Windows Vista: Start - Control Panel - Windows Update - Change Settings

(4) Windows XP: Right-click My Computer icon - Properties - Automatic Updates

(5) OS-X: Go to http://support.apple.com and search (upper right corner) with keywords…security updates

B. Notes:

(1) I recommend you set these updates to automatically install every day. Choose a time of day that your computer is most likely to be turned on. If your system is turned off and you miss some updates, they will automatically be downloaded and installed the next time your system is on at the time of the update.

C. General information:

(1) Windows systems: Go to http://update.microsoft.com and follow directions on screen

(2) Apple systems: Go to http://support.apple.com/kb/HT1338 and follow directions

6. Website Encryption

A. http:// vs. https://

(1) http = contains general (non personal) information only

(2) https = contains (or may contain) personal information
Click on padlock icon for more info at an https Website (such as Site Certificate details by Verisign or another reputable certification agency. Note: On Websites where private or sensitive information is being transmitted, if you see a message indicating "There is a problem with this website's security certificate" then this website isn't properly registered with Verisign (or other certification agency) and you should proceed cautiously because this website **MAY** not be legitimate.

7. Misc.

A. Best to pay with credit card (rather than a debit card).

(1) Using a credit card limits your exposure to $50 (federal law); with a debit card you could be liable up to the balance of your checking account.

(2) Some people prefer to use a low-limit credit card for online transactions.

(3) You have the opportunity to initiate a "charge back" with your credit card carrier.

B. Erasing data -- some free and some fee

(1) Eraser: http://www.heidi.ie

(2) Secure IT: http://www.cypherix.com

(3) LSoft's Active KillDisk: http://www.killdisk.com

(4) CCleaner: http://www.piriform.com/ccleaner

C. Cookies -- A cookie is a small piece of text data sent from a website and stored in a user's web browser when the user visits that website. Cookies cannot carry viruses and cannot install malware on your computer but can create privacy concerns for users. For more information about cookies, go to:

http://en.wikipedia.org/wiki/HTTP_cookie
http://www.onguardonline.gov/articles/0042-cookies-leaving-trail-web

"Instead of waiting for someone to steal my identity, I'm going to auction it on eBay!"

D. Be sure you are at the Website address you really want. Some scammers include the name of a legitimate company in a portion of the Web address, making you think you are really going to the company Website. Examples:
(1) http://www.paypal.com
The domain paypal.com is stored on a server called "www"
(2) http://paypal.money.com
The domain is money.com and it is stored on a server (computer) called paypal (not the same as being at paypal.com)
(3) http://www.company.com/paypal
The domain is company.com and the "/paypal" portion refers to a folder stored on the server. This technique is used to make you think that this Website is related to PayPal.

In addition, be careful when you type in a Web address. Occasionally, a misspelled Web address will take you to a Website that looks like your destination but is really owned by a "typo-squatter" -- someone who creates a fake Website that looks like another.

E. Back up your data files periodically in the event of a security breach that may delete files. For more information, check http://www.iteachyou.com/backup.pdf

F. Find references to your name on the Internet: http://www.iteachyou.com/findname.htm

G. **Never** participate in email chain letters. Most of these have an email tracker attached that automatically forwards each email address back to the original sender. Good security software on your computer should keep this from being a problem for you, but not necessarily others on the route of the chain letter.

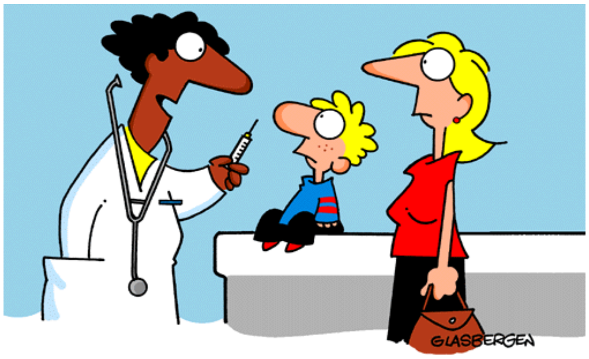
H. Beware of services that **guarantee** to protect your identity. A guarantee is not possible. They can, however, watch carefully for activity that appears to be or lead to identity theft. Examples of such services include Protect My ID (http://www.protectmyid.com) and LifeLock (http://www.lifelock.com).

I. If you use Facebook, MySpace, or other social networking sites, it is safest to restrict access to personal information (or postings) by adjusting settings in your Account/Profile. For example, in Facebook, you should change all settings to "Friends Only" so only people you have pre-approved can see your information. Also in Facebook, click Account-Account Settings-Account Security. Place a checkmark by 'Browse Facebook on a secure…' and click Save.

J. Websites with additional helpful information about protecting yourself online:
(1) http://www.komando.com/top10/privacy.asp
(2) Internet Crime Complaint Center -- http://www.ic3.gov
This site is run by the FBI and the National White Collar Crime Center.
(3) Identity Theft Resource Center -- http://www.idtheftcenter.org -- San Diego office (858) 693-7935
(4) National Fraud Information Center -- http://www.fraud.org
(5) Medical privacy -- http://www.patientprivacyrights.org
(6) Privacy Rights Clearinghouse -- http://www.privacyrights.org (based in San Diego).
(7) Electronic Privacy Information Center -- http://www.epic.org
(8) Privacy Choice -- http://www.privacychoice.org

Summary of Most-Critical Protection Tasks

1. Install quality security software (see #1)
2. Watch carefully for phishing emails (see #2).
3. If you have a wireless network, be sure it is encrypted (secure) (see #4).
4. Set Windows operating system to update automatically (see #5).



"Don't think of it as getting a flu shot.
Think of it as installing virus protection software."