INTERNET SAFETY CLASS

Useful Links

Software to check if your PC is part of a botnet (and disconnect from it): http://www.bothunter.net/

The InfoWorld expert guide to Web browser security:
http://www.infoworld.com/d/security-central/the-infoworld-expert-guide-web-browser-security-892

Check what information about you is available on the Internet: use any normal search engine, plus these:

http://pipl.com/ http://www.spokeo.com/
http://www.intelius.com/ http://people.yahoo.com/

(use a search engine to find more people searches)

For software help on passwords, do a search on: "password generator" and "digital wallet", plus these:
https://lastpass.com/ http://keepass.info/ https://agilebits.com/onepassword

U.S. Government – Best Practices for Keeping Your Home Network Secure (PDF)
https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_BestPracticesForKeepingYourHomeNetworkSecure.pdf

Free Wi-Fi can cost you (Chicago Tribune article)
http://articles.chicagotribune.com/2011-05-31/travel/sc-trav-0531-business-class-20110531_1_unsecured-network-free-wi-fi-virtual-private-network

Frightening story of what can happen with insufficiently secured wireless network:

http://www.wired.com/threatlevel/2011/07/hacking-neighbor-from-hell/

http://blogs.computerworld.com/18636/defending_a_wifi_network

Passwords: Tips for Better Security (InformationWeek article)
http://www.informationweek.com/news/security/client/231000545

Who Bears Online Fraud Burden: Bank or Business: (InformationWeek article)
http://www.informationweek.com/news/smb/security/231000381

Windows Operating System Infection Rates (Microsoft Security Intelligence Report)
http://download.microsoft.com/download/1/A/E/1AE5C1D8-8874-481B-94F8-57B41D4E8965/Microsoft_Security_Intelligence_Report_Volume_17_English.pdf

Good story on botnets and their herders
http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html

Online Internet Safety class
http://www.gcflearnfree.org/internetsafety

Password cracking
http://arstechnica.com/security/2013/08/thereisnofatebutwhatwemake-turbo-charged-cracking-comes-to-long-passwords/

Use 'Common Sense'

1. Remember, *If it seems too good to be true, it usually is* **and** *There's no such thing as a free lunch.*
2. Use available security measure such as firewalls, anti-virus software, anti-spyware software, etc.
3. Regularly scan the entire system for malicious software and immediately after any suspicious encounters
4. If you don't know the sender, don't follow links or open attachments
5. If you know the sender, be aware that person's account may have been taken over **before** clicking
6. Don't respond to unsolicited advertisements in e-mails
7. Don't allow your natural curiosity cause you to do something foolish
8. Avoid sites that offer free or inexpensive movies/videos/porn/software – they are very dangerous
9. If an OK/Cancel dialog box pops up while browsing, try to close it. If that doesn't work, close the browser. If that doesn't work, shut down the computing device any way you can. NEVER click the OK.
10. If you get an offer to 'fix' your computer while browsing, follow the directions for an OK/dialog box. NEVER accept such offers.

Protecting your privacy

1. Configure your browser to refuse third-party cookies
2. Configure your browser to delete cookies and history when closing
3. Use 'private browsing' (typically under the 'Tools' menu)
4. If using the Firefox browser, consider these good add-ons for privacy:
    a. https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/
    b. https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/
    c. https://addons.mozilla.org/en-US/firefox/addon/ghostery/
    d. https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/
5. Disable location detection
6. Use available privacy settings on social media sites
7. Be very careful about content of blogs/tweets/posts – remember it is nearly impossible to remove information once it has been placed on the Internet

Typing special characters

Use the Alt key plus these four digits ON THE 10-key pad of a full-sized keyboard to get:									
0188	¼	0215	×	0163	£	0156	Œ	0222	Þ
0189	½	0177	±	0165	¥	0167	§	0223	ß
0247	÷	0162	¢	0191	¿	0182	¶	0230	æ
http://symbolcodes.tlt.psu.edu/accents/codealt.html for a much bigger list									

Using Credit Cards

1. Don't use a wireless connection unless you **know** it is secure **and** encrypted.
2. Be sure the URL is preceded by http**s**:// – not just http://
3. Consider using 'private browsing'
4. Understand how URLs work
    a. Don't go to an address with all numbers ('raw' internet address)
    b. Do read the URL carefully for substituted or extra letters
    c. Beware reading only part of a URL – read each section between dots from RIGHT to LEFT
    d. Be aware that the visible text is NOT the actual link target
5. Consider using one browser only for financial and sensitive information
6. Consider using a LiveCD – the LiveCD List at http://www.livecdlist.com/ is huge (300+ last count) with info about each

Wireless Network Security Essentials

1. **Never** use a wireless router as-is out-of-the-box – it is configured to be as easy as possible to use – and the least secure
2. Encryption should always be enabled
    a. Use 128-bit encryption rather than 64-bit encryption
    b. Do **not** use WEP (Wired Equivalent Privacy) – it is not secure
    c. WPA (Wi-Fi Protected Access) is usually adequate, BUT
    d. WPA2-AES (WPA2-CCMP) is best
3. Use a unique network name – not the default name of the router, not the name of the owner; it is better to use something hard to guess, i.e., not SMITHFAMILY
4. Do not broadcast the SSID (Service Set IDentifier) – your neighbor should not be able to see you have a wireless network
5. DHCP (Dynamic Host Configuration Protocol) should be **disabled** (not normal for most routers)
6. Use static NAT (Network Address Translation) addresses
7. Restrict access to specific MAC (Media Access Control) addresses (a unique number present in network interface cards and other network devices) – but don't rely on this because MAC addresses can be spoofed
8. You should have a firewall enabled on the wireless router, not just on your PC and other computing devices
9. Administrator accounts for the wireless router should be accessible only from within your network – if you can access it from your work or from Starbucks, so can someone else. (Typically called 'Remote Administration' or 'Remote Management' – turn it OFF.)
10. If the wireless has a 'Guest Network' feature, use it. Make the password for it – i.e. what guests and visitors need to use it different than the password for your private wireless network.
11. If you don't know how to do these things, pay someone to do it for you (or never use the network for sensitive information)