Computer and Information Security Topics

Most of text in this document is copied from the following websites:

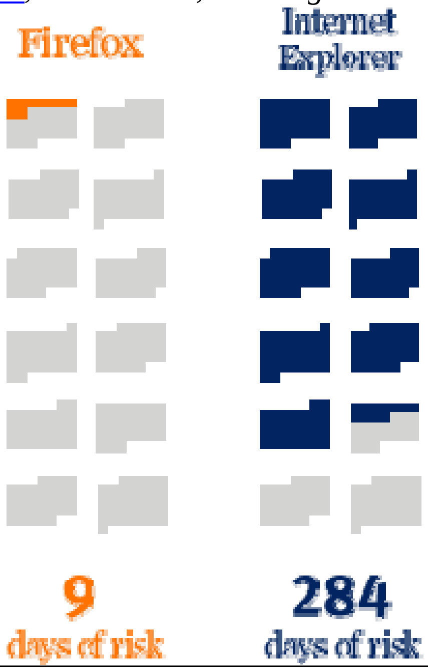
- http://www.cert.org/tech_tips/
- http://computer.howstuffworks.com/security-channel.htm
- http://netsecurity.about.com/cs/compsecurity101/
- http://staysafeonline.org/practices/
- http://wikipedia.org/

	Topic	Explanation Vulnerability
1.	**Accessing the system: Turn off computer**	**Turn off your computer** or disconnect from the network when not in use. Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.
2.	**Anti-virus software**	**Install and maintain anti-virus software**. There are plenty of great anti-virus software packages available. This software checks for known viruses by scanning your computer periodically. Most will also check for viruses on incoming email. It is important to update the software as well though. New viruses are discovered almost daily. At least once a week you should check the web site of the vendor that makes your anti-virus software to see if there is an update available.
3.	**Cookies**	A **cookie** is a piece of text that a Web server can store on a user's hard disk. Cookies allow a Web site to store information on a user's machine and later retrieve it. Possible problem: People often share machines. Any machine that is used in a public area, and many machines used in an office environment or at home, are shared by multiple people. Let's say that you use a public machine (in a library, for example) to purchase something from an online store. The store will leave a cookie on the machine, and someone could later try to purchase something from the store using your account.
4.	**Digital signatures**	A **digital signature** is a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is **authentic**. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it. Digital signatures rely on certain types of **encryption** to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures.
5.	**Downloading free software**	**Piggybacked software installation -** Some applications -- particularly peer-to-peer file-sharing clients -- will install spyware as a part of their standard install. This is especially true of the "free" versions that are advertised as an alternative to software you have to buy. There's no such thing as a free lunch.
6.	**Electronic payment**	The main drawbacks to electronic payments are concerns over privacy and the possibility of identity theft. Fortunately, there are many safeguards available to protect your sensitive personal information from falling into the wrong hands. You can defend yourself against identity theft by using virus protection software and a firewall on your computer. You should also make sure that you send your credit card information over a secure server. Your Internet browser will notify you when a server is secure by showing a lock or key icon. In addition, the URL

		on a secure site is usually designated by the prefix "https" instead of "http." Retailers do their part by using data encryption, which codes your information in such a way that only the key holder can decode it.
7.	**E-mail : Opening unknown or suspicious mail**	**Do not open unknown or suspicious email**. Many viruses and worms use what is called “social engineering”. That is, they attempt to trick you into becoming a participant in the process. The latest viruses can “spoof” the sending email address so that it looks like it is coming from someone other than the computer that infected it. If an email is not from someone you know, it is usually best to simply delete it without looking at it. If the email appears to be from someone you know, you should read the message carefully before opening any attached files. Viruses and worms often have bad English and poor grammar. Consider whether the person you know would really have written that message or forwarded you the attached file. If in doubt, contact that person you know to confirm they truly sent it before opening the attachment.
8.	**E-mail: Anti-spam filter**	Your email software may help you avoid viruses by giving you the ability to filter certain types of spam. It's up to you to activate the filter.
9.	**E-mail: E-mail Encryption**	**Encrypting your email** will keep all but the most dedicated hackers from intercepting and reading your private communications. Using a personal email certificate like the one freely available from Thawte you can digitally sign your email so that recipients can verify that it’s really from you as well as encrypt your messages so that only the intended recipients can view it. Comodo is another company offering free digital certificates for personal use. You can obtain your free certificate by filling out a very short and simple registration form.
10.	**E-mail: opening E-mail attachments**	**Don't open unknown email attachments** Before opening any email attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs. If you must open an attachment before you can verify the source, we suggest the following procedure: 1. be sure your virus definitions are up-to-date (see "Use virus protection software") 2. save the file to your hard disk 3. scan the file using your antivirus software 4. open the file For additional protection, you can disconnect your computer's network connection before opening the file. Following these steps will reduce, but not wholly eliminate, the chance that any malicious code contained in the attachment might spread from your computer to others.
11.	**Encryption**	Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.
12.	**Firewall**	A **firewall** provides a strong barrier between your private network and the Internet. You can set firewalls to restrict the number of open ports, what type of packets are passed through and which protocols are allowed through.
13.	**Instant Messaging (IM)**	Because using **IM software** requires you to have a service connected to the Internet on an open port, it offers an attack vector for hackers. The IM software tends to have security flaws and vulnerabilities that allow for malicious attacks.
14.	**Internet browser**	It is difficult to determine whether browsers such as Firefox, Opera and Apple‘s Safari are really safer than Internet Explorer (IE). However, since IE is the most

		used browser, most hackers concentrate on IE. See also **WEB browser**
15.	**Pass words: Change Password Enforcement**	**Enforce stronger passwords:** Rather than relying on every user of the computer to understand and follow the instructions above, you can configure Microsoft Windows password policies so that Windows will not accept passwords that don't meet the minimum requirements.
16.	**Passwords: Change Password**	**Change your passwords**. You should change your password at least every 30 to 60 days. You should also not re-use a password for at least a year.
17.	**Passwords: Easy Passwords**	**Do not use personal information**. You should never use personal information as a part of your password. It is very easy for someone to guess things like your last name, pet's name, child's birth date and other similar details.
18.	**Passwords: Easy Passwords**	Do not use real words. There are tools available to help attackers guess your password. With today's computing power, it doesn't take long to try every word in the dictionary and find your password, so it is best if you do not use real words for your password.
19.	**Passwords: Easy Passwords**	**Mix different character types**. You can make a password much more secure by mixing different types of characters. Use some uppercase letters along with lowercase letters, numbers and even special characters such as '&' or '%'.
20.	**Passwords: Easy Passwords**	**Use a passphrase**. Rather than trying to remember a password created using various character types which is also not a word from the dictionary, you can use a passphrase. Think up a sentence or a line from a song or poem that you like and create a password using the first letter from each word.
21.	**Passwords: Password Managers**	**Use a password management tool**. Another way to store and remember passwords securely is to use some sort of password management tool. These tools maintain a list of usernames and passwords in encrypted form. Some will even automatically fill in the username and password information on sites and applications.
22.	**Passwords: Single Password**	**Use different passwords**. You should use a different username and password for each login or application you are trying to protect. That way if one gets compromised the others are still safe. Another approach which is less secure, but provides a fair tradeoff between security and convenience, is to use one username and password for sites and applications that don't need the extra security, but use unique usernames and more secure passwords on sites such as your bank or credit card companies.
23.	**Passwords: Storing and Remembering Passwords Securely**	There are a number of **tools available to help you securely store and remember your passwords and usernames** without keeping a cheat sheet in your wallet, a list in your desk drawer or yellow sticky notes on your monitor. Check out the links below for more details: RoboForm Password Safe Whisper 32 KeyWallet
24.	**Peer-to-peer fie sharing networks**	The fact that computers participate on one of these **P2P networks** means they must have certain ports open on their networks or computers. In this case they generally will have at least one folder on their computer shared out as well. Having open ports and open file shares offers another prime target for malicious developers to exploit. **Piggybacked software installation -** Some applications -- particularly peer-to-peer file-sharing clients -- will install spyware as a part of their standard install.
25.	**Scripting (JAVA,**	Using **JavaScript** you could take user input, perform calculations, display the current date and time and a slew of other things that make the page change over

		time or unique from user to user. This sort of dynamic content or content that was unique to the user made the World Wide Web much more interesting than simply viewing static pages. Always the goal has been to find more and better ways to dynamically update the web page with information that is new or unique to the user. To do this the scripting languages had to be able to pull information from the client computer or sometimes from databases housed on the server. The scripts are small programs that execute within the HTML code. And therein lays the problem. If a legitimate web site or web developer can use active scripting like JavaScript, VBScript or ActiveX to dynamically gather information from your computer to aid in displaying custom data, then a malicious developer can use that same functionality against you. It didn't take too long for malicious developers to figure out that they could create active scripting programs within web sites that would plant Trojan horse files or viruses on your computer or copy your personal information back to them.
26.	**Spyware**	**Spyware** is a category of computer programs that attach themselves to your operating system in nefarious ways. They can suck the life out of your computer's processing power. They are designed to track your Internet habits, nag you with unwanted sales offers or generate traffic for their host Web site. According to recent estimates, more than two-thirds of all personal computers are infected with some kind of spyware. Spyware usually gets onto your machine because of something you do, like clicking a button on a pop-up window, installing a software package or agreeing to add functionality to your Web browser.
27.	**Spyware: Anti-Spyware Tools**	**Anti-Spyware Tools**. Even with antivirus software, firewalls and other protective measures some spyware or adware may eventually make it through to your system. The makers of AdAware Pro, Lavasoft, have a version available for free for personal use. AdAware will not monitor in real time, but you can manually scan your system periodically to detect and remove any spyware. Another excellent choice is Spybot Search & Destroy which is also available for free.
28.	**System maintenance: Installing security patches**	**Keep your computer patched against known vulnerabilities**. Almost as often as new viruses are discovered, new vulnerabilities are discovered as well. Many times they are in the operating system (like Windows), but vulnerabilities are also found in tools like your web browser, email software and other 3rd party tools. Left unpatched, these vulnerabilities can be exploited by hackers to obtain access and control of your computer. Staying up to date can be difficult. Some vendors, such as Microsoft, have automated utilities that check for updates and notify you. Other vendors may have an email mailing list you can join so they can notify you of any new updates. If your vendor doesn't offer one of these solutions, you may just need to periodically visit their support web site to check for any new patches or updates.
29.	**Telephone modem**	Modem connections represent a major, back-door security threat to the security of your LAN. **Modem connections** can be used by outside intruders (hackers) to gain unmonitored and unauthorized access into your corporate data network
30.	**VPN**	A **VPN is a private network** that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.
31.	**Browser**	A **web browser** is a software application which enables a user to display

		and interact with text, images, videos, music and other information typically located on a Web page at a website on the World Wide Web or a local area network. There are several web browsers: Internet Explorer, Firefox, Apple Safari etc. Internet Explorer is the most used browser and therefore the most vulnerable to attacks. "At risk" defined as publicly available exploits with no patch. Source: "Internet Explorer users Unsafe for 284 Days in 2006", Brian Krebs, *Washington Post*, 1/4/2007 
32.	**Web sites, web pages, social network sites containing personal information**	You've read it here, and you know it well: **using your real, primary email address anywhere on the Web** puts it at risk of being picked up by spammers. And once an email address is in the hands of one spammer, your Inbox is sure to be filled with lots of not-so-delicious spam every day. Spammers use special programs that extract email addresses from Web sites and Usenet postings.
33.	**Wireless network**	**Wireless networks** add an extra level of security complexity compared to wired networks. Whereas wired networks send electrical signals or pulses of light through cable, wireless radio signals propagate through the air and are naturally easier to intercept. Signals from most wireless LANs (WLANs) pass through exterior walls and into nearby streets or parking lots.
34.	**Wireless network: encryption**	One of the ways to ensure unauthorized users do not eavesdrop on your **wireless network** is to encrypt your wireless data.