

Internet Safety



Table of Contents		
➤ Basic Safety Tips	Pg. 2
○ 9 Rules to Follow	Pg. 2
➤ Anti-Virus Downloads	Pg. 2
➤ Facebook/MySpace	Pg. 3
○ Facebook Security	Pg. 3
○ Twitter Security	Pg. 4
➤ Online Shopping	Pg. 5
○ Basic Tips	Pg. 5
○ PayPal	Pg. 5
➤ Internet Jargon	Pg. 6

Basic Safety Tips

9 Rules to Follow

- 1. Never give any personal information to anyone you meet online.** That means first or last names, phone numbers, passwords, birth dates or years, or credit card information.
- 2. Never meet up with anyone you don't already know.** Don't tell anyone your schedule; don't say where you'll be hanging out. No party announcements. People are often not who they say they are
- 3. Don't fill out any "fun" questionnaires that are forwarded to you, even if they're from your friends.** Remember, you're in a world where everything can get forwarded. All those personal things about you could land in the hands of someone who could use them to harm you.
 - Note that once you put something on the internet, it's basically always there. Search engines will make caches of websites, so even if you remove something from online, there's probably still a record of it somewhere.
- 4. Make sure you know everyone on your buddy list.** If you haven't met the people face-to-face, they may not be who they pretend to be.
 - Avoid public chat rooms. Many people try to phish for information from these sites. Also, many sexual predators use chat rooms to pursue sexual encounters.
- 5. Do not have to answer emails or IMs from people you don't know.**
 - Don't answer emails saying you've won the lottery or you have inherited money.
 - Don't ever give passwords or credit card information online.
- 6. Remember, there's no such thing as "private" on the Internet.** You may think so, but it's not true. People can find anything they want — and keep what you post — forever.
- 7. Be careful about posting pictures of yourself (And don't post anything you wouldn't want your mother, children, boss, or college advisor to see).** Pictures with identifiers like where you go to school can be shopping lists for online predators.
- 8. Don't download content from sites you don't trust.** Some downloads can result in viruses or an extraction of personal information.
- 9. Never share your password with ANYONE!** A legitimate company will never solicit your password through email or telephone.

Internet Vocabulary

Phishing: the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Downloading: By downloading something (like a music file, document or photo) you are transferring information from the internet to your computer

Antivirus Downloads

Antivirus Software: software you can download or a program that searches your computer for known or potential viruses.

There are many different free antivirus programs you can download and install onto your computer. Some reputable free ones include:

- Adaware: http://www.lavasoft.com/products/ad_aware_free.php
- Avast: <http://www.avast.com/free-antivirus-download>
- AVG: <http://free.avg.com/us-en/download>
- Spyware Doctor: <http://www.pctools.com/spyware-doctor>

Twitter and Facebook Safety

Twitter and Facebook are two very popular social networking sites. These can be great places to keep in contact with friends, but they can also be dangerous if you don't take certain safety precautions.

- Utilize your Privacy Settings. Both Twitter and Facebook give you the opportunities to change your privacy settings. This can allow only a limited amount of people to see your information and alter security levels.



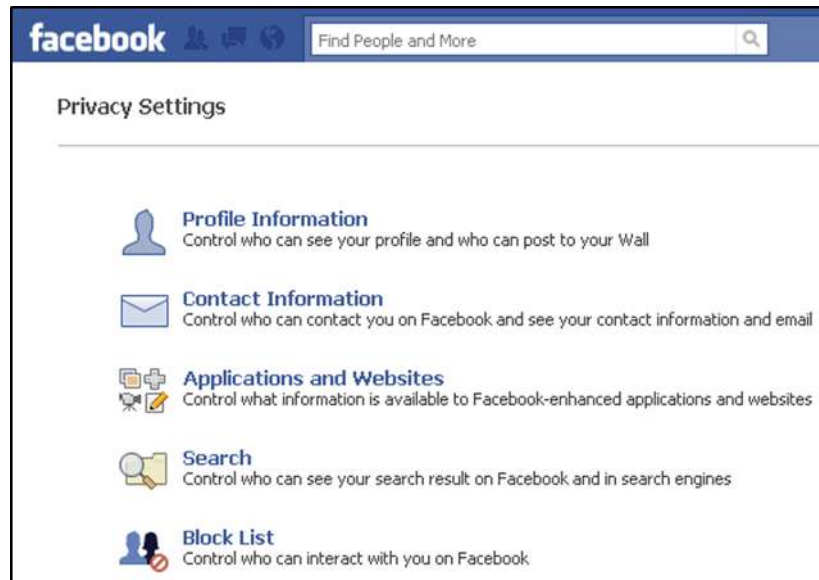
- To change Privacy Settings on **Twitter**, click on the **Settings** link on the banner.

Then you will be taken to a screen explaining the different things you can change. Clicking on any of the links will take you to the actual page to change those specific settings.

- To change Privacy Settings on **Facebook**, click on the **Account** link on the banner. Then, click on the **Privacy Settings** link.



Then you will be taken to a screen explaining the different things you can change. Clicking on any of the links will take you to the actual page to change those specific settings.



Guidelines to follow on social networking sites:

- **Restrict your profile to only people you have met in person.** Setting your profile to “private” allows only trusted friends to view your information. You still have to be careful what you post, but it's less likely that someone you don't know will view your personal profile.
- **Only visit profiles of people you know.** Stick with the profiles of people you know and trust. It makes it less likely you'll run into someone who'll try to hurt you, but it also helps protect you from downloading viruses and malware to your computer.
- **Never post anything on your profile that you wouldn't say in public.** Your profile isn't completely private, no matter how many settings you change. Twitter can be especially dangerous because anyone can “follow” you without your permission, so watching what you say is very important. More and more colleges and employers are looking to see what you're doing online, so think before you post.
- **Not everything you read is true.** Have you ever said something that wasn't true? It happens all of the time. Don't believe everything you read. People pretend to be older or younger and sometimes guys pretend to be girls and girls pretend to be guys. You just can't believe everything you read, even if you want to. This is also important to keep in mind when accepting online friend requests. Sometimes, people pretend to know you or say they read your profile and you have a lot in common. Just ignore these requests.
- **NEVER share personal information such as phone numbers, addresses, social security numbers etc. online.** It's dangerous, plain and simple.

Online Shopping

Basic Tips

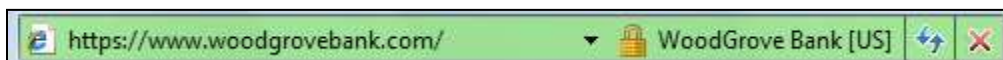
- **Make sure the business is legitimate.** Buy from reputable stores and sellers. If you have doubts, choose another company. Find out what other shoppers say. Sites like Epinions.com or BizRate have customer evaluations which can help you determine a company's legitimacy.
- **Look for third-party seals of approval.** Companies can put these seals on their sites if they abide by a set of rigorous standards—such as how personal information can be used. Two seals to look for are the “Better Business Bureau Online” and “TRUSTe Certified Privacy.” If you see the seals, click them to make sure they link to the organization that created them. Some unscrupulous merchants will put these logos on their sites without permission.



- **Use a filter that warns you of suspicious Web sites.** Browser filters warn you about reported phishing sites and block you from visiting them. For example, two browser filters are the SmartScreen Filter in Internet Explorer 8 and the Phishing Filter in Internet Explorer 7.

- **Keep your Web browser updated.** Internet Explorer 7 and 8 provide another layer of protection with sites that use Extended Validation (EV) Secure Sockets Layer (SSL) Certificates. An EV SSL certificate not only helps ensure that the communication with a Web site is secure, it also includes information about the owner of the Web site, which has been identified by the Certification Authority (CA) issuing the SSL Certificate. The address bar turns green and has both https and the closed padlock.

- **Make sure the Web site uses encryption.** On the Web page where you enter your credit card or other personal information, look for an "s" after http in the Web address of that page. It should read: https://. Also make sure there is a tiny closed padlock in the address bar, or on the lower right corner of the window.



- **Encryption:** Encryption is a security measure that scrambles data as it traverses the Internet

PayPal

<http://www.paypal.com>

- **PayPal is the world's most popular "middleman service" for online purchasing.** Where moneygrams and wire transfers were the standard in the 20th century, today over 99 million Internet users prefer to use PayPal to send money to each other via email. PayPal has become such a convenient and trusted way to transfer money online, 95% of eBay's purchases go through PayPal.

- **How PayPal Works.** As an online financial transaction broker, PayPal lets people send money to each other's email addresses. At no time will either party see the other's credit card or bank information. Similar to an escrow service, PayPal acts as the middleman holder of money. Through its policies,

practices, and business integrity, PayPal has earned the trust of both parties. With multiple guarantees in place, buyers and sellers entrust PayPal with their credit card and bank information. PayPal keeps that private customer information secret. Then, while "blinded" from the other party's confidential information, strangers safely send money to each other through PayPal and email.

• **PayPal Requirements.** You do not need any special technology or business license to have a paypal account. The only requirements are:

- A valid email address.
- A valid credit card or bank account.

How Safe is Paypal?

• **Although no system is 100% foolproof, PayPal has designed many checks and balances into its system to keep errors and fraud to a bare minimum.** You won't find another online financial institution that's better at protecting its customers than PayPal. By utilizing the very latest in secure technology and employing a large team of experts in all areas of online safety, PayPal continues to be a leader in safe online payments around the world.

• **PayPal is guaranteed against fraud and identity theft.** PayPal guarantees 100% protection against unauthorized payments from your account. Every transaction is confirmed by email to the PayPal account holder. Any transaction you wish to dispute will give you access to a 24/7 support team of analysts who will sort out your problem for you.

• **eBay purchases can also be insured up to \$1000 through PayPal.** A service called "PayPal Buyer Protection" is another way that PayPal will certify that certain sellers are trustworthy.

• **PayPal's Anti-Fraud Team works 24/7** Using sophisticated risk models and advanced technology, the team is able to detect, and often predict, suspicious activity to help eliminate identity theft. The anti-fraud team's sole job is to make every PayPal transaction as safe and seamless as possible.

Internet Jargon

• **BLOG or WEB LOG:** A blog (short for "web log") is a type of web page that offers a series of posted items (short articles, photos, diary entries, etc.). Blogs usually include a searchable archive of old postings. Blogs have become a common medium for communication in professional, political, news, trendy, and other specialized web communities.

• **BOOKMARKS/FAVORITES:** All major web browsers include a way to store links to sites you wish to return to. Netscape, Mozilla, and Firefox use the term Bookmarks. The equivalent in Internet Explorer (IE) is called a "Favorite."

- To create a bookmark, click on BOOKMARKS or FAVORITES, then ADD. Or left-click on and drag the little bookmark icon to the place you want a new bookmark filed. To visit a bookmarked site,

click on **BOOKMARKS** and select the site from the list. Most browsers also include commands to Import and Export lists of bookmarks.

- **BROWSE:** To browse through a page, exploring what's there and seeing where the links take you, is a bit like window shopping. When you browse, you have to guess which words and links on the page pertain to your interests. The opposite of browsing is searching.
- **BROWSERS:** Software programs that enable you to view web pages and other documents on the Internet. They "translate" HTML-encoded files into the text, images, sounds, and other features you see. The most commonly used browsers are Microsoft Internet Explorer (often called IE), Firefox, Mozilla, Safari, Opera, and Chrome.
- **CACHE:** In browsers, "cache" is used to identify a space where web pages you have visited are stored in your computer. A copy of documents you retrieve is stored in cache. When you use **GO**, **BACK**, or any other means to revisit a document, the browser first checks to see if it is in cache and will retrieve it from there because it is much faster than retrieving it from the server.
- **CACHED LINK:** In search results from Google, Yahoo! Search, and some other search engines, there is usually a **Cached link** which allows you to view the version of a page that the search engine has stored in its database. The live page on the web might differ from this cached copy, because the cached copy dates from whenever the search engine's "spider" last visited the page and detected modified content.
- **CASE SENSITIVE:** Capital letters (upper case) retrieve only upper case. Most search tools are not case sensitive or only respond to initial capitals, as in proper names. It is always safe to key all lower case (no capitals), because lower case will always retrieve upper case.
- **COOKIE:** A message from a **WEB SERVER** computer, sent to and stored by your browser on your computer. The main use for cookies is to provide customized Web pages according to a profile of your interests. When you log onto a "customize" type of invitation on a Web page and fill in your name and other information, this may result in a cookie on your computer which that Web page will access to appear to "know" you and provide what you want. If you fill out these forms, you may also receive e-mail and other solicitation independent of cookies.
- **DOMAIN NAME, DOMAIN NAME SERVER (DNS) ENTRY:** Any of these terms refers to the initial part of a URL, down to the first /, where the domain and name of the host or **SERVER** computer are listed (most often in reversed order, name first, then domain). The domain name gives you who "published" a page, made it public by putting it on the Web.
- **DOWNLOAD:** To copy something from a primary source to a more peripheral one, as in saving something found on the Web (currently located on its server) to diskette or to a file on your local hard drive.
- **FIND:** Tool in most browsers to search for word(s) keyed in document in screen only. Useful to locate a term in a long document. Can be invoked by the keyboard command, **CTRL+F** (**CMD+F** on a Macintosh).

- **HISTORY, Search History:** Available by using the combined keystrokes CTRL + H. You can set how many days your browser retains history in Edit | Preferences, or in Tools | Options.
- **IP Address or IP Number:** (Internet Protocol number or address). A unique number consisting of 4 parts separated by dots, e.g. 165.113.245.2 Every machine that is on the Internet has a unique IP address. If a machine does not have an IP number, it is not really on the Internet. Most machines also have one or more Domain Names that are easier for people to remember.
- **KEYWORD(S):** A word searched for in a search command. Keywords are searched in any order. Use spaces to separate keywords in simple keyword searching.
- **LINK:** The URL imbedded in another document, so that if you click on the highlighted text or button referring to the link, you retrieve the outside URL. If you search the field "link:", you retrieve on text in these imbedded URLs which you do not see in the documents.
- **RSS or RSS feeds:** By subscribing to an RSS feed, you are alerted to new additions to the feed since you last read it. In order to read RSS feeds, you must use a "feed reader," which formats the XML code into an easily readable format/
- **SEARCH:** You can search any individual web page using the CTRL-F command (CMD-F on a Macintosh). Many websites also offer search boxes that let you search all the pages in the site, or records in its database. Searching is usually the most efficient way to find information, but sometimes you can find things by browsing that you might miss otherwise because you might not think of the "right" term to search by.
- **SITE or WEB-SITE:** This term is often used to mean "web page," but there is supposed to be a difference. A web page is a single entity, one URL, one file that you might find on the Web. A "site," properly speaking, is a location or gathering or center for a bunch of related pages linked to from that site.
- **SPIDERS:** Computer robot programs, referred to sometimes as "crawlers" or "knowledge-bots" or "knowbots" that are used by search engines to roam the World Wide Web via the Internet, visit sites and databases, and keep the search engine database of web pages up to date. They obtain new pages, update known pages, and delete obsolete ones. Their findings are then integrated into the "home" database.
- **URL**
 - *Uniform Resource Locator.* The unique address of any Web document. May be keyed in a browser's OPEN or LOCATION / GO TO box to retrieve a document. There is a logic the layout of a URL:

- *Anatomy of a URL:*

Type of file	Domain name	Path or directory on the computer to this file	Name of file
http://	www.lib.berkeley.edu/	TeachingLib/Guides/Internet/	FindInfo.html

Sources

Internet Safety is a topic that has been greatly discussed and there are many wonderful sources online to learn about it. Below is a list of places that contributed to this tutorial. Please note that some of this tutorial has been directly copied/pasted from these sites.

- <http://www.common sense.com/internet-safety-tips/tips-for-kids.php>
- text.netalert.gov.au/advice/publications/guides/a_teachers_guide_to_internet_safety/glossary.html
- <http://familyinternet.about.com/od/computingsafetyprivacy/a/TeenMySpace.htm>
- http://www.microsoft.com/protect/fraud/finances/shopping_us.aspx
- http://netforbeginners.about.com/od/ebay101/ss/paypal101_4.htm