

# SAFE SURFING FOR ADULTS!!

While there is a wealth of information available for teaching children how to safely use the internet, the sources of such information for adults is far more limited. Most of the information found on the internet is related to companies marketing various products to protect you. They do not usually give you the information needed to protect YOURSELF!

## *Some of the General Concepts*

### **Common Sense**

The first of thing to do is use common sense. The internet is not much different from walking down a street, stopping in shops, talking to people you know and often talking to those you do not know.

In that situation, it is likely that you will give out some personal information to people that you know. We all do it. However, we are likely to 'pick and choose' what information we give based upon how well we know the individual.

The same should hold true for your internet travels.

Be careful who you give information to and stop to evaluate why that particular information is required. If it does not make sense to you that the 'individual/company' you are dealing with would be asking for that information, then you may want to look a bit more closely by contacting the requester through email or telephone (look for a "Contact Us" link on the page).

Never give out your password. The only people you should be discussing your password with are those where the password applies (i.e., your email account, a place online where you frequently shop that requires a password). Those people probably already know more about your password than you do. You may have to ask their assistance in obtaining your password or in having a new password generated by them, but they should not ask you for your password unless it is in response to a direct inquiry by you or in a situation where you have tried, unsuccessfully, to enter a password. Most of these places have a link that you click in order to have them assist you in generating a new or obtaining an old password.

The other situation where you may be required to give a password (other than where it is generally required for access to a site or email account) is if you select to change your password. In this case, you have already access the correct site and are simply modifying the information that agency has for you. It is not a situation where someone you do not know is trying to get you to give your password.

Be particularly wary of emails coming to you that tell you to click a link on the email to go and change or update your personal information. Never use the reply button on one of these emails to try to contact the company for additional information. For example, if I were contacted in an email that seems to have come from my email host, Verizon, I go to the official Verizon website and look for a Contact Us link. That will provide me with the information needed to contact an official Verizon source via email, telephone, or even 'snail mail'. Often, I copy and paste the text of the letter I received and ask them to verify whether this is legitimate or not. If someone is trying to take advantage of their customers online, the company is quite happy to know about the 'scam' (if they don't know already) and, if the request is legitimate, they will let you know and verify the contact information/process needed to safely complete the transfer of information.

Some of the things you should not be giving out on the internet in general are:

1. Your full name and/or address.

2. Your telephone number.
3. Your social security number.
4. Your credit card numbers.

Additionally, refrain from giving out information such as the names and/or ages of your children, spouse, etc. This includes email addresses. Many people find it useful and safer to use one browser (Mozilla Firefox, Internet Explorer, Netscape Navigator, etc.) and one specific email address (gmail, verizon, yahoo, etc.) for all sales based transactions. I tend to do the same thing with requests for information when I do research. Not only does this make sure that personal information is less likely to be 'leaked' out to the internet, it also means that I know exactly where to look for specific information or copies of sales receipts (you should always maintain a printed copy for all internet sales).

### ***Email and attachments:***

The best rule is if you do not know who sent it to you, then do not open it or download it. If you are going to be working with a group of people on a project, it is easy to set up a "Subject Line" that you all agree upon as the one to use for all dialog related to the topic. This can be just a few letters and symbols at the beginning of the subject line or it can be entire words and phrases. If you think an email may be from one of these people, but you are not sure. It only take a few minutes to send a fresh (not a reply) email to that individual and get them to verify that they are the source or to resend it with the "Subject Line" that you had agreed upon.

### ***Keep your computer and program (application) software up-to-date!***

Everyone gets tired of all those microsoft updates (except for Mac users of course). However, they happen for a reason. Many of the updates you will receive (or have to check for) are because a problem has been identified as a hacker used some piece of the program to get into the system. When this happens, people report the problems and the software provider begins making modification so as to block the intruder. If you do not keep your operating system (OS) and program software up-to-date, you will not have the protections in place and you are more vulnerable to attack by hackers whose goal is to get into your system for information or to create havoc!

### ***Don't believe your eyes on first sight. Looking twice can save you a lot of grief!***

One of the most common ruses in use right now is where you go to a website and all of a sudden you find yourself looking at something that appears to be a legitimate warning from your computer that the website is trying to infect your computer. These sites will tell you to click on a link that then tries to download a file to your computer. One of the first things that I do when I see these is to check the bar on my computer showing what programs are open. If this is a legitimate warning from your computer you will see the antivirus, firewall, spyware protection program, or windows program that is prompting you listed. If it is not there, then a valid window IS NOT open. Don't click on anything, simply close the site. In fact, simply close the site anyway, do not click on any of the links on the page, use the close button and do not save the site anywhere. If there is a legitimate problem, the proper software on your computer generating the notice will remain up whether you are on the internet or not.

This whole process is designed to feed on fear. People see a problem and react almost by instinct. DO NOT freak out! Stay calm. The most recent example of this that I have found came up on a google search – Note that since I blogged on this particular site a few days ago, it has been removed from the Internet:

I just did a google search on Virginia delegate voting records and the second site on the list was:

[\*Virginia Delegates Voting Record\*](#)

*Virginia Delegates Voting Record. Portillo's Beef Nutrition Facts » Cat Hair Loss Hock » Poor Nutrition Fetal Dead » Body Hair Growth In Men ...*

*[brendenstickel.jsrqidyxw.cc/virginia\\_delegates\\_voting\\_record.html](http://brendenstickel.jsrqidyxw.cc/virginia_delegates_voting_record.html) - 3 hours ago - [Similar](#)*

\*\*\*Note the part I put in italics: "Cat Hair Loss Hock...." This was my first indication that something was not quite right! Read before you click. If it looks like things are not quite right, then don't click on it. I mean what has cat hair, fetal dead, and body hair got to do with Delegate voting records.

Also note the link listed at the bottom....who ever heard of brendenstickel as an entrance page to a Virginia site? I beefed up my security and clicked:

If you click on that link you are taken to a site that is related to something called searchandprotect.net. You will immediately get noticed that your computer has a serious virus problem and is immediate danger.

The authors of the webpage have designed webpages that look almost identical to the Windows security page warning you would see if you have an actual problem. You will be prompted to continue by clicking buttons in order to save your computer.

DON'T DO IT!!!! I stayed only long enough to verify that this was a simulation of the security prompts before I hightailed it out of there.

When in doubt, close the site, close all of your browser windows and run your anti-virus and/or anti-spyware. If you are then showing problems, let your programs handle them or give a call for help to someone you trust! The odds are excellent that, if you did not click on any of the buttons they tried to trick you into clicking, your computer will test clean, just like mine did.

### ***Shopper Beware!***

Just because a website looks nice and professional does not mean it is so. Be sure that the site you go to belongs to a valid retail business. You can often determine this by recognition of a name (Sears, Amazon, etc.) or by doing a google search on the business name. Putting the name of the business in quotation marks forces google to search for that exact name, not look-a-likes designed to trick you. (For an example, do a google search on "joe pie's lavender shop" and the search will come back noting that NO RESULTS WERE FOUND.

Most businesses will have a domain name that matches the name of their business. For instance, if you plan on shopping at Amazon, they have a web address of <http://www.amazon.com>. Banks and businesses generally follow this format. Additionally, look at the bottom of your browser and you should see some place where you can find a small 'lock'. It should be locked. This is how you can tell if you are on a secured site. A secured site means that the site you are interacting with has provided safety features that protect any information you may give them, such as name, address, credit card number, etc.

Any business website that does not provide you with access to information such as a legitimate street address or phone number could have something to hide. Stay away from those that only have PO Box numbers unless you know them.

Look the website over carefully for items such as:

- contact information
- customer service
- return policies
- a telephone number to use in lieu of the internet ordering option

### ***Copyrights Apply!***

Be very careful that if you quote a site or use any of the audio/video/photo information on a site that you obtain information. It is perfectly legal to write up your comments and then give a link to the site that has the information. Just do not copy and paste something that someone else has done!

### ***Sources of More Information:***

- [Washington State Office of the Attorney General](#) has a nice site discussing Internet Safety
- [The USAA Educational Foundation](#) – provides a 16 page .pdf document that provides definitions as well as a discussion of many safety steps to take on the internet (for both adults and children).
- [Lovetoknow's – Internet Safety Adult](#) site provides a lot of useful information as well as links to more specific articles
- [The Internet National Fraud Information Center](#) can help you stay up-to-date on the latest scams and issues on the internet, on the phone, and in local stores.
- [The Federal Trade Commission - Identity Theft](#) site provides a wealth of information concerning identity theft and how to protect yourself from it.