210115: There was a time that I was excited to get home from work and get online. There was so much to see and learn and do. I even learned how to write HTML 3 then HTML 4 by attending classes in a chat room. The big jump in my learning HTML came when I learned that I could right click a page and select to see the page source. By doing this I could see how other coders did their work and learn from it. However, as the internet has matured, I have seen a trend that is upsetting and even dangerous! The dangers arise from an insidious behavior I have noticed coming from Microsoft and Google.

The first sign of trouble arose from the battle between Microsoft and “Sun Microsystems, Inc.”, the authors of Java. I am sure there are a lot of folks, like myself, who have enjoyed the fun of Java Applets. I even had a few Java pages on my website that were just for fun. Microsoft, on the other hand could not get Sun Microsystems to sell them the Java rights. Eventually in 2001, Microsoft decided to demonize the use of Java. (https://en.wikipedia.org/wiki/Microsoft_Java_Virtual_Machine) It is my suspicion that Microsoft was behind creating bad code that acted like hacker code that would make some users afraid of Java. Today, any form of Java on a website or machine has been treated as a virus. I suspect this was all by design to get rid of the competition and to bring Microsoft closer to controlling all HTML code and browsers. Now even Windows itself will not allow one to open a page that is using a Java Applet! That really pisses me off that I cannot even view stuff that is locally on my own machine!

The latest attack is on the use of Shock Wave. Any Shock Wave apps or extensions are immediately treated as a virus and deleted from a person’s browser without the user’s choice!

This too is all by design to force people into using browsers that are heavily monitored by both Microsoft and Google. I say this because the new HTML 5 and the latest CSS 3 are both designed to snoop on anyone visiting a page that is written or conforms to the new code. Of course a savvy page coder can prevent the snooping by having their code sourced to locally uploaded apps and scripts. Every server has a system in place that records what machine address has visited or accessed what page, scripts, and content posted on that server. The new CSS 3 tries to get coders to access scripts that are on the CSS servers (w3.org). By doing this the CSS folks have access to a seriously large data base of machine addresses. I can only guess this information is primarily for gathering advertising resources. But the uses can be endless and may even be used as individual behavioral analysis.

Browser use is also being funneled into using “Snooping” browsers such as “Google Chrome” and “Microsoft Edge”. Right now users are warned they have an unsecure browser if they are not using either Chrome or Edge. It is a scare tactic to make people switch. Why do they want folks to switch? The best answer I can come up with is that these two browsers are scripted to call home and report where and what the user is doing on their browser. Anyone using these browsers can attest that their spam mail and pop up ads has increased after switching to either one of these browsers.

What about Firefox? The jury is still out about Firefox. Apparently it is not being flagged at the moment as an unsafe browser by MS nor Google. So who knows if they are onboard with the big snoop conspiracy? There are still a lot of websites that don’t flag SeaMonkey either, however, some sites do warn about using SeaMonkey since it has popup protection and erases all traces of where one has been once the browser is closed.

Microsoft’s claims regarding their new HTML 5 and CSS 3 are actually false. They claim that using CSS scripting reduces the amount of coding on a page, however, they don’t mention and the total page load of CSS documents along with the parent page far exceeds the page load of a single written coded page. Again, it is a deception in order to get coders on board to using the newer code. Using the newer code gives Microsoft and Google access to everyone’s browsing business. In order to force coders to use the newer HTML 5 code, Microsoft has even changed a lot of the older HTML 4 and older call-outs. Eventually with everyone using the newer browsers, they will not be able to visit the web pages that are written in the former HTML 4 and older code. Most likely, they will be tagged by the browsers as unsafe or some such BS! Similar to how they tag a page that may have a java applet embedded. I have never seen a bad java applet so it makes me seriously doubt Microsoft’s claims since they did never get a “free” user agreement with Sun Microsystems! They decided to demonize them instead!

Java script is still being used, but it appears it is being rewritten by Microsoft to fit their needs. At any rate, watching Microsoft and Google get more and more control of the internet users makes my spidey sense tingle!