

Medical Office Systems, LLC

August 2010 Newsletter

Miscellaneous Topics

This month, I have some miscellaneous topics that don't rate a full newsletter by themselves, yet are worth mentioning nonetheless. I will discuss an article by The Wall Street Journal, information about the Alureon Trojan/Rootkit, and antenna problems with the Apple I-Phone 4.

Missed or lost a newsletter? You can always get back issues in Adobe PDF format online at my website - www.MedOfficeSystems.com/newsletter_tips.htm. If you have any questions about this or any prior newsletters, please call me at 630-852-1736 or 630-373-7429.

Topic 1: The Wall Street Journal

Don't get me wrong, I like The Wall Street Journal. However, last week's technology feature article, "The Web's New Gold Mine" was about privacy issues that can occur while using big-name websites. In short, the article reviewed the top 50 most popular websites for the presence of tracking software ("cookies") that can pinpoint website users down to the local geographic and individual level (your age, gender, address, income, - and maybe even your name!). It is a good article, but I felt it was slightly over the top in terms of the hysteria level. Further, one portion was slightly misleading, and they left out two suggestions I feel are essential

The availability of user-level detail is pretty scary; previously the typical tracking software could generically group at a higher level, such as "female near Chicago, Illinois" or "male interested in golf". How the tracking software can get to a more detailed level is interesting. Without going into the minutiae of the process, let's just say they "triangulate" into your identity by coordinating information on your PC, publicly available data sources, and what you search for.

The biggest coordination of data comes from social websites like FaceBook, MySpace, Twitter, or LinkedIn, to name a few. There is a lot of personal data in those sites. Think about it, in LinkedIn you have addresses, phone numbers, current and past employers. That, plus the cookies left on your computer from web site visits equals trouble.

The part of the article I thought was misleading was the suggestion to turn off cookies completely. I had to laugh, as almost 80% of websites require cookies to work correctly. So if you follow the advice of The Wall Street Journal, you will not be able to use any search engine, shopping sites, airplane ticket sites, or even The Wall Street Journal's website without having all or part of the site fail to work properly. I don't like it that cookies are so prevalent, but they are necessary for most of the features and functions of the Internet to function.

How then, does one limit this data gathering? The best way to prevent or limit tracking is don't put so much personal data out there on the web in the first place. For any website that requires a login or registration, put in only the bare minimum data you can. Most social websites have privacy settings that limit data gathering. Weak though they may be, make sure that you use the "Keep Private" features enabled within those sites.

Next, enable the "Delete cookies on exit" feature of your web browser. I don't have space to cover every type of browser, but it's usually under the "Tools", "Options" or "Settings" menus. This will erase your session after you exit your browser, and limit the cookies that can be searched for data. Likewise, in the same "Tools, Options" menu area, disable the "autocomplete" feature that remembers logins and passwords. If you want to get really fancy, you can use your browser's anonymous mode, or an anonymous proxy website such as www.anonymouse.org.

Reprint permission granted, provided the following appears on each page:
Copyright © 2010, Medical Office Systems, L.L.C. - www.medofficesystems.com

Phone: 630-852-1736

john@medofficesystems.com

Fax: 630-214-4565

Topic #2: Alureon Trojan/Rootkit

In the past month or so, I have had a lot of experience with this bug - Alureon is the most sophisticated in recent memory. It combines elements of a Trojan horse (poses as a virus remover, but is a virus itself) and a rootkit (modifies Windows so it is hidden from the system itself). If you get Alureon, and try to use the "System Restore" feature of Windows, don't bother - Alureon has already infected that, and restoring will just put a new copy back on the system. Even more sophistication is evident as Alureon has learned how to disable most anti-virus programs. Needless to say, Alureon is very, very difficult to remove once it infects a computer. Infections, left untreated, will render the computer inoperable: you'll have to pull out the original CD's and re-install from a clean slate.

Alureon gets on your system in the usual methods: it can come from an infected, but otherwise legitimate website, "free" gaming, music, video or other pop culture, coupon or "bargain shopper" sites. If you are surfing the web and you get an unexpected pop-up window warning that your computer is infected and dire consequences will happen if you don't click "Scan Now", just shut down your computer immediately. Hit the power button and hold it until it is completely off. Don't try to click anything, don't try to use it, and for heaven's sake, don't click "Buy Now"!

After rebooting, update and run your virus scanner immediately. Don't use the computer until the scan is complete. If you notice any strange behavior, like you searched for shoes, but got sites that sell cars, pharmaceuticals or whatever else, you may still be infected. You can try to remove it by using the MalwareBytes scanner - Malwarebytes is one of the best at removing Alureon in its early stages. You can download it from www.malwarebytes.org, install it, and run a full scan. If that does not work, you can also try "ComboFix", available from Cnet.com. ComboFix is very effective, but I must warn you that using ComboFix runs the risk of disabling the computer if it finds a core operating system file that is infected. Or, you could call me at 630-373-7429.

Topic #3: Apple iPhone 4

I like Apple products, but every now and then, even the best companies mess up. This is the case with the Apple iPhone4. The details are wrapped in the arcane, murky science of antenna design, but I can tell you two simple facts:

1. The iPhone 4 has a metal band antenna that wraps around the edge of the device.
2. Anything that touches a metal antenna will change reception in unpredictable ways, mostly for the worse.

It is well documented that cell phones specifically are the most affected by antenna design due to the small form factor. Why Apple chose to put a metal antenna around the outside edge of the phone is beyond reckoning - I guess they were going for elegant looks over performance.

Most disturbing about this incident is Apple's initial denials that there was any problem at all. Their subsequent backpedaling, and blaming users who held it with their fingers touching the edge... borders on the ridiculous. So how then is one supposed to hold the phone? Regardless, Apple has capitulated to the facts and issued a fix: a rubber "bumper" sleeve that goes around the phone, insulating the metal strip from the human hand.

If you have questions, comments, or debate counterpoints about these current topics or any prior topics in my newsletters, please call me at the phone number below, or contact me by email. Thanks for listening!
