



Bexar County IT News

August 2013



Computer Plug-in Devices: Beware!



They come in all shapes and sizes. They may be cute and clever looking or just plain boring in their appearance. They long ago replaced the floppy disk for storing and transporting data and they can hold different quantities of information - from a few megabytes up to very large amounts. (A flash drive with one-terabyte of storage capacity was shown at the 2013 Consumer Electronics Show in January.) The fact of the matter is that these devices (flash drives, ThumbDrives, jump drives, memory sticks, etc.) are commonly found in today's information technology toolbox.

But despite all their usefulness and convenience they are just like any other tool. If they are not carefully used or are used by someone with nefarious intentions, the amount of damage caused by simply plugging in one of these devices can be devastating. Of course, in addition to being used to infect your system with a virus or malware, they can be used to steal sensitive data.

It is widely believed, for example, that Edward Snowden recently heisted major National Security Agency secret data on a humble flash drive he slipped into his pocket and carried home from work one day.

And the Stuxnet worm, one of the world's most sophisticated cyber weapons, which severely damaged Iran's nuclear program in 2010 was reportedly implanted by use of a memory stick to gain access to the target.



Another example: the Conficker malware, first detected in November 2008 that infected more than 15 million computers and tens of thousands of corporations. The origin of the infection was an unauthorized USB flash drive that contained a worm. It took a determined (and very expensive) global effort by many security companies to shut that down.

More often than not, however, the damage done by these devices is brought on by someone who has no ulterior motives - someone who just doesn't practice good cyber security.

In a recent "penetration test" run by a security firm (Idappcom) for the U.S. Department of Homeland Security it was proven that the major weakness which would allow hackers to gain access to "secure" computer systems revolves around the human factor. DHS staff deliberately dropped data disks and USB flash drives in federal agency and contractor parking lots. A full sixty percent (60%) of those planted data devices were plugged into office computers; the employees were apparently just curious to see what was on them. And if the data device had an official logo on it, it was inserted into the network 90 percent of the time!



In February 2013, South Korea's largest IT security vendor, AhnLab, Inc. conducted a survey of

(Continued on page 2)

(Continued from page 1)

300 IT professionals - many of them working in security. The study revealed that 78% of those surveyed admitted to picking up and plugging in USB flash drives found abandoned or lying around! And it was discovered that the "found" USB drives often included viruses, rootkits, and bot software.

How can organizations combat this ever-present threat? Obviously, there is a clear cut need to have comprehensive security policies and procedures in place which will govern the safe and restricted use of these devices. Additionally, there are software programs available such as USB port-blocking software, malware detection devices and USB devices with hardware-based encryption. These things are proper and essential in maintaining the cyber security of an organization.

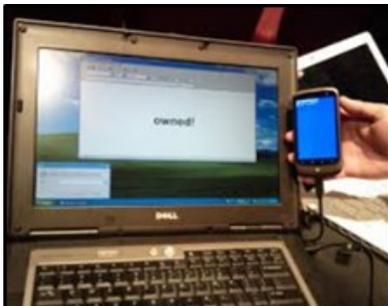


However, the **first, most important step toward establishing a secure environment is to make employees mindful of the potential dangers involved.** In general, computer users are not sufficiently aware that the use of unsecured USB-type equipment can present a real risk to their machine and, ultimately, their entire organization.

So, the bottom line: do not use any plug-in device that holds the slightest possibility of having been infected from outside sources, whether it came from home or a third party - or you found it in the parking lot! For additional information check out the following websites:

- <http://www.blockmastersecurity.com/top-5-usb-flash-drive-hidden-security-risks/>
- <http://www.cisecurity.org/>
- <http://www.cioinsight.com/security/the-dangers-of-unsecured-usb-drives/>

Other Possible Plug In Devices to Beware of:



Optimizing Your Internet Experience



About cache, cookies, and history

Each time you access a file through your web browser, the browser caches (i.e., stores) it. By doing this, the browser doesn't have to newly retrieve files (including any images) from the remote web site each time you click **Back** or **Forward**. You should periodically clear the cache to allow your browser to function more efficiently.

A cookie is a file created by a web browser, at the request of a web site, that is then stored on a computer. These files typically store user-specific information such as selections in a form, shopping cart contents, or authentication data. Browsers will normally clear cookies that reach a certain age, but clearing them manually may solve problems with web sites or your browser.

A browser's history is a log of sites that you visit. When you press a browser's **Back** button, you are moving back one entry in the history log. Browsers will normally clear the history at regular intervals, but you should clear it manually for privacy.

How to delete cache, cookies, and history

Internet Explorer 7

1. From the **Tools** menu in the upper right, select **Delete Browsing History...** .
 - (a) To delete your cache, click **Delete files...** .
 - (b) To delete your cookies, click **Delete cookies...** .
 - (c) To delete your history, click **Delete history...** .
2. Click **Close**, and then click **OK** to exit.

How to Access Your Outlook Webmail Account

If you ever feel the need to access you work email from home here are some steps that might help with those last minute issues that cannot wait until the next business day.

- In Internet Explore type <https://webmail.bexar.org/owa> in the address bar.
- Select this is a public or shared computer (See Picture Example)
- Type you username with Bexar\ before it
- Click the Log On button on the bottom left

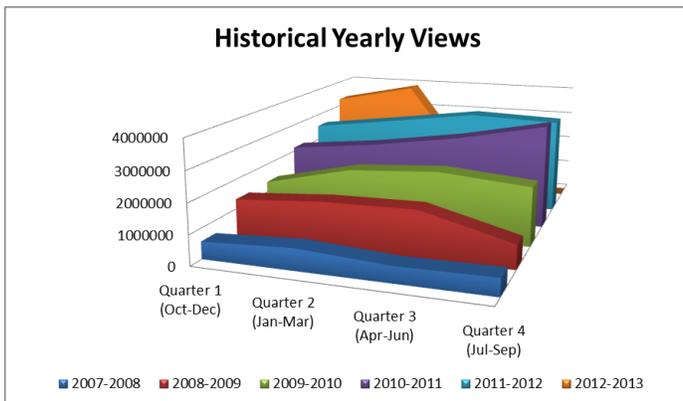
BexarCLAW - Law Enforcement's New Tool

BCIT has incorporated a new tool for law enforcement called BexarCLAW (Bexar Criminal Listings & Active Warrants). It's a search engine that allows the DA's, Sherriff's office, and squad cars to conduct background searches on individuals. Users can do Basic searches, which allows them to enter keyword(s) and the system will return any record that has a match. For more detailed searches, users have the option to use an advanced search engine. With the advance searches the users have the ability to search on specific fields like name, DOB, driver's license, address, and general demographics (height, weight, sex, race, and eye color). This will give the user the ability to acquire more refined results.

BexarCLAW results return a list of individuals, along with a mug shot, that meets the users search criteria. Users can click on a mug shot and they will be direct to a page with detail information about the individual. This page displays general demographic information, all mug shots and previous booking history. If the individual has active warrants they will be displayed as well. BexarCLAW gives the user the capability to see all criminal history on one screen. Officers that are out in the field will have more knowledge of an individual's criminal background. This gives the officer an advantage and better prepares them when dealing with individuals. Since BexarCLAW was implemented last year it has caught the interest of SAPD and they have been using the system, as well as Schertz PD and other outside agencies. BexarCLAW is another example of how Bexar County is maximizing the use of technology to provide better services.

A History of Bexar County's Web Analytics

Quarters	2007-2008	2008-2009	2009-2010	2010-2011	2011-2012	2012-2013
1 st Quarter (Oct-Dec)	576,348	1,329,323	1,360,508	2,139,218	2,548,200	3,272,716
2 nd Quarter (Jan-Mar)	726,849	1,543,455	2,053,956	2,470,823	2,952,597	3,902,266
3 rd Quarter (Apr-Jun)	540,834	1,593,260	2,252,704	2,933,240	3,370,260	
4 th Quarter (Jul-Sep)	575,000	806,065	2,002,448	3,552,454	3,272,174	
Yearly Totals	2,419,031	5,263,103	7,669,616	11,095,735	12,143,231	



Top Webpages In the Last Month

1. Homepage
2. Magistrate Search
3. Civil Litigant Search
4. Court Records Search
5. District Clerk website
6. County Courts
7. Justices of the Peace website
8. District Courts
9. Bexar County eServices
10. Probate Courts