Technology by Design

Email: marketing@tbyd.ca
Phone: 204-800-3165

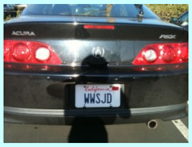
July 2013 Edition

TECH TIPS

VISIT OUR WEBSITE/BLOG: tbyd.ca
LIKE US ON FACEBOOK: facebook.com/TechnologybyDesign FOLLOW US ON TWITTER: @techbyd

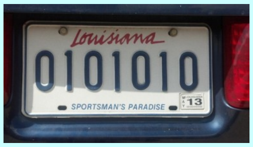
Geek Your Ride

It's July, and with July comes road trips. Check out some of the geeked-out license plates you may see on your travels this summer…



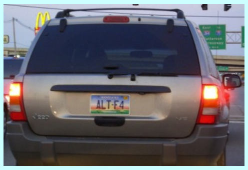
1. **Steve Jobs #1 Fan**
"What Would Steve Jobs Do". I'm guessing he wouldn't get this license plate…or maybe he would…

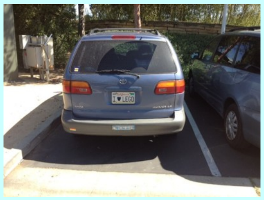
2. **Sheldon Cooper's License Plate**
If he drove, of course



3. **Family Unity**
Forget the cling-on family on the back window, advertise your family unit stating how many XX chromosomes and how many XY chromosomes.

4. **Keyboard Nerd**
By the van, I'm guessing this geek is married…which is amazing in itself





5. **Lego Lover**

6. **Microsoft Fan**
I'm guessing this wasn't Steve Jobs' car

McAfee Software Founder Resurfaces

Eccentric software pioneer John McAfee, who helped create the anti-virus software industry, made the news last year when he fled his home on a tropical island in Belize, claiming that police in the Central American nation wanted to frame him for murder.

McAfee fled his home in Belize, disguised himself and went into hiding after his American neighbor was fatally shot in November. He secretly made his way to Guatemala but was deported to Miami in December. He reports that police in Belize were persecuting him because he refused to pay $2 million in bribes, and that the extortion attempt occurred after armed soldiers shot his dog, smashed up his property and falsely accused him of running a methamphetamine lab. Belize police report that McAfee is "a person of interest" in the ongoing murder investigation, and is wanted for questioning.

Now, McAfee has resurfaced on YouTube, producing videos in which he lashes out and the anti-virus software, which bears his name, in a profanity-laced video. In the video, he complains about the difficulties of removing McAfee anti-virus software from computers, and he reads what he claims are letters of complaint from those who have used it. McAfee states the software was "beautiful" before it "fell" out of his hands. In the video, McAfee uses a lot of profanity, appears to snort a powder and fire a gun into a computer, is undressed and pawed by a group of young women. McAfee states he did it all to mock the media's unfair portrayal of him as a mad man.

<u>JULY TRIVIA QUESTION:</u>

How much was Judy Garland paid for The Wizard of Oz?

- $10/day - $35/week - $100/day - $240/week

Email your answer to: answer@tbyd.cafor your chance to **win coffee & donuts** delivered to your workplace!

<u>**PLUS**</u>, Your company will be featured in next month's issue of TechTips, on our blog, and our Facebook page!

<u>**Your feature will reach over 2000 other people!**</u>

June 2013 Trivia Winner:

Ralph at Treaty Aboriginal Rights Research Centre of Manitoba Inc.!

The Treaty Aboriginal Rights Research Centre, or T.A.R.R. Centre, has been in business since 1975. They are a non-profit company, that works directly for most of Manitoba's First Nations.

T.A.R.R. Centre provides historical research services to 51 First Nations of Manitoba. Through the years, the focus has been on Aboriginal rights such as Treaty land entitlement, Treaty rights, hunting, fishing, trapping and gathering rights, and on Indian lands (reserve alienations, surrenders, leases and expropriations). T.A.R.R. has been a part of the creation of the Specific Claims Tribunal (2006), with the power to make binding decisions on Land Claims of value up to $150 Million.

All Member First Nations are welcome to access their resources. Non-First Nation members can receive photocopies at cost.

There are 3 T.A.R.R. locations: Scanterbury, Thompson, and Winnipeg. Head Office is located at Brokenhead Ojibway Nation, Scanterbury, MB.

Technology by Design is currently responsible for handling all IT-related issues for T.A.R.R. Centre.

For more information, please contact Ralph at 204-943-6456, or email Ralph@tarr.mb.ca.

Don't forget your entry for this month's trivia for a chance to win coffee & donuts…delivered to your workplace!

PLUS, Your company will be featured In next month's issue of TechTips, on our blog, Twitter, and our Facebook page!

Your feature will reach over 2000 potential customers!!

5 Fun Facts From the Latest NSA Leak

After a brief intermission, the Guardian newspaper has resumed its publication of leaked NSA documents. The latest provides a peek at the secret rules the US government follows for collecting data on US people. Among the most interesting:

1. The NSA generally destroys communication of US persons that are collected incidental to collecting data on foreign individuals—unless the communication is encrypted, which means that encrypted email and text communications involving US persons that are collected by the NSA in the course of conducting bulk collection would be retained by the agency. So, using the "wrong" ecryption program, you could popular with the NSA.

2. The NSA maintains a massive database of US email addresses and phone numbers. The agency says it does this only to help determine who is a US citizen and therefore make sure that it's not 'accidentally' spying on those people.

3. The NSA also maintains a database of information incidentally collected from GSM and Home Location Registers to determine when a foreign person being targeted has entered into the US.

4. When the NSA does pick up purely domestic communications, it can still use or pass the intercepted call or email to the FBI or other federal agencies if there is evidence of a crime or a national security leak.

5. If the NSA intercepts data between an attorney and client, it will still be retained, but will be marked for special handling, such that the portion of the communication related to national security is segregated from the rest of the communication. This applies, however, only when the client is known to be under criminal indictment. The rules do not mention what the NSA does if the clients are communicating with their attorneys on other cases.

A Final Fun Fact: The NSA still uses magnetic tapes for their backup. Which, if you've been reading our literature, has a fail rate of 100%!

I wonder if the NSA and Google Street Views have talked…

Mutant Silkworms

In my 2nd reference to Sheldon Cooper in Big Bang Theory: His glow-in-the-dark fish had nothing on these silkworms.

Silkworms in a Japanese lab are busy spinning glow-in-the-dark silks. No, this isn't the 1st time this has happened. BUT it is the 1st time the worms have done so without any dietary intervention. Previously, in order for silkworms to produce these silks, they had to be fed rainbow-coloured dyes. The new & improved silkworms have been genetically engineered to produce fluorescent silks in shades of red, orange, and green.

Now, scientists have tweaked the silk production process, and made it possible to turn these somewhat freakish threads into useable fabrics. The new silks glow under florescent light, however are just slightly weaker than silks that are normally used for fabrics.

This isn't the first time that scientists have genetically modified silkworms to suit their needs. Silkworms have previously been modified to produce substances such as spider silk, human collagen proteins, and glowing proteins.

Batman Theme Song Re-Mastered!

If you have a few minutes on your hands, and have nothing else to do, check out this version of the Batman Theme Song...played with real bat sounds.

Some people have wayyyy too much time on their hands! AND, just a wild guess here, doesn't have a girlfriend.

Check out the theme song: http://www.youtube.com/watch?v=N95tCG4IeWY&feature=youtu.be

Street View: Google Hits Roadblock

Google has been given 35 days by the UK information Commissioner's Office to delete any remaining data it "mistakenly collected" while taking pictures for its Street View service, or face criminal proceedings.

Inquiries into Google's data gathering began in 2010 when it was leaked that an engineer had written software code to gather information from unsecured wi-fi networks. Cars taking pictures for the company's popular Street View service were used to capture the information.

Google had previously pledged to destroy all data it had collected, but admitted last year that they had "accidentally" retained the additional discs.

The investigation was re-opened last year after further revelations about the data taken from wi-fi networks. During that inquiry, additional discs containing private data were found.

Included in the data collected: complete email messages, email headings, instant messages and their content, logging-in credentials, medical listings and legal infractions, information in relation to online dating and visits to pornographic sites.

The company was fined $25,000 by the US Federal Communications Commission in April of 2012.

Moral of the story: secure your wi-fi network!

BURNING COMPUTER QUESTION ??

Email our Resident Geek!
We'll even translate the answer from Geek-lish to English, so the it actually helps!

Email your question to: geek@tbyd.ca
Check our blog for the answer: tbyd.ca

TechTip Postcard

Insider Tips and Secrets to Get The MOST Out of Your Computer

Declare Freedom From Computer Problems!

The 5 Biggest Mistakes Winnipeg Business Owners Make With Their Computer Network That Cost Them Time, Money and Aggravation

Want to avoid the most common and expensive computer problems most Winnipeg business owners experience? Then read on! We've compiled a list of 5 things you should be doing to save yourself a lot of

1. **Have an automated off-site back-up system in place.** I cannot stress the importance of this enough. Having an off-site back-up of your data will be the equivalent of wearing a seatbelt in a major accident. You don't think much about it until you need it, and then, you will thank your lucky stars you had it in place.

2. **Centralize your data on your server.** At one time, servers only made sense for large organizations because of their high cost and complexity. But today, there are very affordable and easy-to-implement server systems designed specifically for any size small business. A server will not only speed up your network, but it will also make backups easier, allow secure remote access to allow you and your employees to work from home or on the road, and make it much easier to share documents, databases, and printers.

3. **Keep your anti-virus software up-to-date, and perform weekly spyware scans.** Almost everyone understands the importance of anti-virus software, but many businesses still do not perform weekly spyware sweeps. Spyware can cause a host of problems that include slowing down your systems, pop-up ads, and even identity theft.

4. **Create an acceptable use policy and enforce it!** One of the biggest threats to your network are your employees! Although that sounds harsh, it is true. Employees can accidentally introduce viruses and spyware through innocent activities online such as checking their Gmail account, downloading photos, or visiting phishing websites set up by online criminals. There are several great programs available for monitoring employee activity online. If you would like a recommendation for your specific situation, call our office.

5. **Perform regular maintenance.** Just like your car, a computer network needs regular maintenance. This includes monitoring of critical components, performance, security patches, and your back-up system. Regular maintenance can dramatically improve the speed and reliability of your network, as well as the security of your data. If you cannot afford to lose data or be down for days, you must perform regular maintenance on your network!

Contact Us NOW If You Want An Easy Way To Make Sure You Aren't Making These 5 Mistakes In Your Business!

204-800-3167 or visit: www.tbyd.ca