

Subject: From Fantasy to Reality - Teens Take "World of Warcraft" into Felony Land



In This Issue

[Darwin Awards](#)

[Hacking Away!](#)

[Background Checks](#)

[Buggy Software](#)

[Living Cellphones](#)



For more than three decades Jean Mignolet has served in law enforcement and private investigation, managing all aspects of general investigative business. She specializes in in-depth background investigations, and has been the top choice for attorneys,

Dear Jean ,

Twas the Season!

The season for the holidays, the parties, the reconnections with friends and loved ones, the shopping, the shipping, the traveling, the cold, the snow, the donations to charity, the gifts, the exhaustion, the drinking, and the building of memories.

Now it's winding to a close. But it was so busy that many of us forgot to look ahead to the new year.

Many of my clients start contacting me in December to discuss their needs for January. This is because the new year often serves as the start for new ventures and projects. These activities require information on wide range of topics -- from the backgrounds of new business partners, to the safety records of different industries, to the crime rate of a new market area.

Don't worry if you haven't had the time for planning. Just give me a call whenever you get going so we can discuss the full range of your needs for the new year.

corporations, small business owners and individuals requiring all types of investigative services. For more information, visit www.Mignolet.com or contact us at investigators@Mignolet.com or 954-523-8737

Quick Links

[Our Website](#)

[Services](#)

Join Our Mailing List!



Stoopidity Roolz!! It's time for this year's Darwin Awards

The annual honor is given to the persons who did the gene pool the biggest service by killing themselves in the most extraordinarily stupid way. Last year's winner was killed by a Coke machine which toppled over on top of him as he was attempting to tip a free soda out. This year's winner was a real rocket scientist...

Read on ... And remember that each of these is a true story.

Semifinalist #1

A young Canadian man, searching for a way of getting drunk cheaply, because he had no money with which to buy alcohol, mixed gasoline with milk. Not surprisingly, this concoction made him ill, and he vomited into the fireplace in his house. This resulting explosion and fire burned his

As always, thank you for your ongoing feedback. Please feel free to submit questions, comments and ideas for future issues.

Best Regards,

Jean Mignolet

ALERTIf you received an e-mail from my email address regarding jewelry or weight loss, please understand that it did not originate from me. My computer expert, Peter Jarvic said that my computers had NOT been violated and therefore the hacker had gotten my e-mail address from someone else's address book. Keep checking your computers for viruses.**



Caveat Emptor: Employment Background Checks

The AP recently ran an article about a job applicant who was required to undergo a background check. The result was that 14 felonies showed up on her record. The problem was that this was not actually her record, but that of someone with a similar name.

Background checks are booming. Employers spend at least \$2 billion making sure they're not hiring an embezzeller, molester, or worse.

But the system of collecting and distributing background checks is flawed, according to the article. The most sensitive information from people's pasts is now bought and sold as a commodity. Computers glean the public

house down, killing both him and his sister.

Semifinalist #2

Three Brazilian men were flying in a light aircraft at low altitude when another plane approached. It appears that they decided to moon the occupants of the other plane, but lost control of their own aircraft and crashed. They were all found dead in the wreckage with their pants around their ankles.

Semifinalist #3

A Virginia man was found dead after he tried to use octopus straps to bungee jump off a 70-foot rail road trestle. Fairfax County police said a fast-food worker, taped a bunch of straps together, wrapped an end around one foot, anchored the other end to the trestle at Lake Accotink Park, jumped and hit the pavement. The length of the cord that he had assembled was greater than the distance between the trestle and the ground,' Police said. They also said the apparent cause of death was 'Major trauma.'

Semifinalist #4

A man in Alabama died from rattlesnake bites. It seems that he and a friend were playing a game of catch, using the rattlesnake as a ball. The friend - no doubt a future Darwin Awards candidate - was hospitalized.

Semifinalist #5

Employees in a warehouse in west Texas noticed the smell of a gas leak. Sensibly, management evacuated the building, extinguishing all potential sources of ignition; lights, power, etc... After the evacuation two technicians from the gas company were dispatched. Upon entering the building, they found they had difficulty navigating in the dark. To their frustration, none of the

files of court systems around the country to retrieve personal data. The breakdown occurs because what they retrieve isn't checked for errors that would be obvious to human eyes.

A recent investigation by The Associated Press included a review of thousands of pages of court filings and interviews with dozens of court officials, data providers, lawyers, victims and regulators. Their results showed the magnitude of the problems.

"The mix-ups can start with a mistake entered into the logs of a law enforcement agency or a court file. The biggest culprits, though, are companies that compile databases using public information," reported AP.

"Another common problem: When a government agency erases a criminal conviction after a designated period of good behavior, many of the commercial databases don't perform the updates required to purge offenses that have been wiped out from public record.

"It hasn't helped that dozens of databases are now run by mom-and-pop businesses with limited resources to monitor the accuracy of the records."

Data on errors in background checks is not available, but class action lawsuits are becoming more frequent as the problem continues to be exposed. AP writes, "In an effort to prevent bad information from being spread, some courts are trying to block the computer programs that background check companies deploy... Virginia, Arizona and New Mexico have installed security software to block automated programs from getting to their courts' sites." Some other states no longer offer wholesale subscriptions to their information.

The situation is complex. There is little consistency among states regarding their policies and approaches to maintaining and distributing the information. Even the FBI database is not completely accurate.

It all comes together as a clear suggestion that background checks should be conducted by a professional with the resources and experience to acquire and interpret the information. Private investigators have the training to conduct background

lights worked. Witnesses later described the sight of one of the technicians reaching into his pocket and retrieving an object that resembled a cigarette lighter. Then the gas in the warehouse exploded, sending pieces of it up to three miles away. Nothing was found of the technicians, but the lighter was virtually untouched. The technician suspected of causing the blast had never been thought of as "bright" by his peers.

And the winner is ...

(As always, the winner receives the award posthumously.)

The Arizona Highway Patrol came upon a pile of smoldering metal embedded in the side of a cliff rising above the road at the apex of a curve. The wreckage resembled the site of an airplane crash, but it was a car. The type of car was unidentifiable at the scene.

Police investigators finally pieced together the mystery. An amateur rocket scientist had somehow gotten hold of a JATO unit (Jet Assisted Take Off, actually a solid-fuel rocket) that is used to give heavy military transport planes an extra 'push' for taking off from short airfields. He had driven his Chevy out into the desert and found a long, straight stretch of road. He attached the JATO unit to the car, jumped in, got up some speed and fired off the JATO.

The facts as best could be determined are that the operator of the 1967 Impala hit the JATO ignition at a distance of approximately 3.0 miles from the crash site. This was established by the scorched and melted asphalt at that location. The JATO, if operating properly, would have reached maximum thrust within 5 seconds, causing the

checks at a variety of levels, including but not limited to criminal activity. Other areas of concern are verifying marital status, litigation histories, academic credentials, and even a physical address. Without a trained professional working on this, the employer is clearly in danger of making decisions by using the wrong information. In these cases there are double losses -- both the employer and the prospective employees suffer.



Buggy, Buggy, Buggy **80 Percent of Software Apps** **Fail Security Tests**

Wired.com reports that "desktop and web applications remain a wasteland of bugs and holes that only a hacker could love"

Most software applications didn't meet a security assessment by Veracode. During the past 18 months the company used an automated analysis of 9,910 applications submitted to Veracode's online security testing platform.

More than 100 different flaw types were examined. One surprising result: applications created by the government fared worse when it came to cross-site scripting and SQL injection flaws, while commercial applications were more often marred by remote-execution flaws. About 75 percent of government web applications had cross-site scripting issues. Cross-site scripting flaws allow an attacker to inject malicious code into a vulnerable web application to obtain sensitive data from users.

"Government is doing worse for cross-site scripting, which is a bad place to be doing worse for," said Chris Wysopal, co-founder and chief technology officer at Veracode.

In the Wired.com article Veracode speculated the bad grade for government might be due to the fact that a lot

Chevy to reach speeds well in excess of 350 mph and continuing at full power for an additional 20-25 seconds. The driver, and soon-to-be pilot, would have experienced G-forces usually reserved for dog fighting F-14 jocks under full afterburners, causing him to become irrelevant for the remainder of the event. However, the automobile remained on the straight highway for about 2.5 miles (15-20 seconds) before the driver applied and completely melted the brakes, blowing the tires and leaving thick rubber marks on the road surface, then becoming airborne for an additional 1.4 miles and impacting the cliff face at a height of 125 feet, leaving a blackened crater 3 feet deep in the rock.

Most of the driver's remains were not recoverable. Epilogue: It has been calculated that this moron attained a ground speed of approximately 420-mph, though much of his voyage was not actually on the ground.



10 Things You Didn't Know Could Be Hacked

1. Kid-Tracking Devices: There are several tiny GPS devices now on the market designed to help parents keep track of their kids, either by hiding the gadgets in the family car or tossing them into a backpack. Unfortunately, many of

of government applications are built with Cold Fusion, a programming language that has a higher incident of cross-site flaws than C, C++, Java and PHP, the languages more prevalently used in commercial-sector software, Wysopal said. The use of Cold Fusion also suggests that government developers may be less-skilled overall than other developers and don't have the same pressures to build secure software that commercial developers have.

"Other industries, if you're in finance or software, you have to deal with your customers [if there is a security flaw]," he said, whereas the government is focused simply on developing applications that meet regulations and fulfill the functions they need to fulfill.

This is the fourth study that Veracode has released, but only the first one that adopted a zero tolerance for cross-site and SQL flaws in their acceptability criteria.

"Even one flaw is going to probably be found and [a victim] is going to make the news, and it's going to have an impact on them one way or another," said Wysopal.

"Commercial software is by no means more secure than government applications, however. Commercial applications just have a prevalence of different kinds of flaws, such as buffer overflow and management issues that could lead to remote-code exploitation by a hacker."

Veracode also found that 3 percent of commercial applications it examined had backdoors - often included by developers for bug testing or diagnostic support - that could be leveraged by an attacker. Data management software and storage software often had backdoors, Wysopal said, but Veracode also found them apps used for transacting financial information and viewing personal health records."

these devices don't have all the security features they should.

2. Cars: As more cars become connected to smartphones and wireless data networks, they present new challenges for automakers and new opportunities for crooks. A Nissan Leaf owner, for example, recently discovered that he could track a car's position and speed using a simple Web-based data-feed program.

3. Landline Voicemail: The U.K. phone-hacking scandal reminded us how easily most cellular carrier's voicemail systems can be accessed. Unfortunately, landline number voicemail systems work the same way. Many providers use a common set of dial-in numbers for voicemail, and many users leave the default password in place or chose a password that's easy to remember - and easy to hack - such as a birthday or a pet's name. If yours is still on the default password, change it.

4. Old Baby Monitors: That second-hand baby monitor may not be such a bargain after all. Security experts used to make a habit of demonstrating how they could tap into the video and audio feeds of numerous nanny cams while driving through suburban neighborhoods.

5. Portable Game Players: Some older consumer electronics devices, such as the original Nintendo DS and the Nintendo DS Lite, will only work with the older, insecure WEP encryption standard in order to access a Wi-Fi network. (All Wi-Fi users should be using the WPA standard instead.)

6. Hands-Free Bluetooth Car Kits: A security testing firm, warns that many Bluetooth devices are easily hacked. Users also often leave phones and other devices vulnerable by failing to change the default device-pairing passwords (such as "0000" or "1234"); be sure to change yours.

7. Your Front Door: Electronic keypads and wireless remote security systems were once only for businesses. Now there are innumerable home electronic security



Old Cellphones Never Die, They Just Continue Telling Your Personal History

Old smartphones leave tons of data for digital dumpster divers. A recent exploration made by a digital forensics company into a handful of phones found in the smartphone secondary market showed how easy it is to glean information from old or lost phones, even if a factory reset has been committed.

An expert from Access Data gave the website Dark Reading information on his findings from his informal research and explained some of the repercussions for corporations and consumers who do not pick, manage, or dispose of their phones wisely.

"I'd guess if you went and grabbed 10 phones [from recycling companies], 60 percent are going to contain data," he said. At the behest of a customer interested in the data lingering on phones sold by used phone resellers and consumers using Craigslist and eBay, he used AccessData's tools to do an in-depth forensics dive into five handsets acquired from this market. The phones were the iPhone 3G, Sanyo 2300, HTC Wildfire, LG Optimus, and HTC Hero. Of those five, the iPhone and the old Sanyo had not been reset and contained what the director called logical data - active account sign-ons, contacts, and calendar information easily usable by any person who turns on the phone.

Even though all of the Android phones had been wiped through a factory reset, four of the five phones also included data that would take someone with forensics tools and knowledge to extract from more hidden storage locations. Some of the details available within those phones included user account information, Social Security numbers, geo-location tags, deleted text

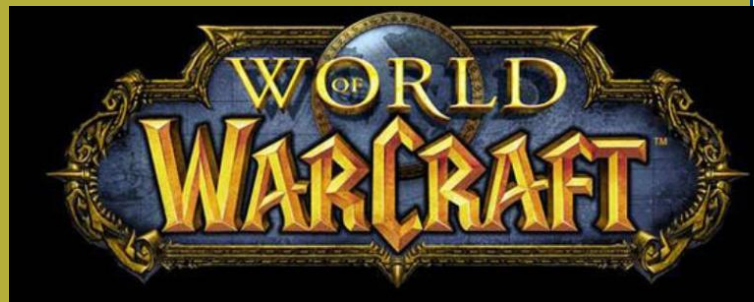
systems, but if they aren't installed correctly, they can make your home more vulnerable to technically adept thieves. Hackers can lift the code, for example, from a stolen smartphone or intercept the wireless signal when you open the door so that they can return later and empty your house.

8. Medical Implants: A researcher demonstrated how he could hack into the wireless signals put out by automatic insulin pumps implanted into human bodies. Three years ago, another team discovered how to turn off a pacemaker by remote control, and companies are now developing wearable "shields" to prevent hacker-induced heart attacks.

9. Garage Door Openers: Don't ever leave the door to your garage unlocked. There are dozens of videos on YouTube showing how to hack garage door openers. Some methods use wires, others simply run through common garage-door codes using smartphones. Poof! Your garage door's open, and anyone can just walk in.

10. Traffic Lights: Believe or not, you can make a red light change to green. Police, fire and emergency vehicles have infrared transmitters that communicate with receivers on traffic lights to do just that. Home versions can be built with a little technical know-how, but a federal law forbids their unauthorized use.

messages, and a resume.



World of Warcraft Confession Uncovers Teen Murderer

Vanity Fair magazine reports that a World of Warcraft confession and other digital evidence allowed the Vancouver Police and the Royal Canadian Mounted Police to solve the murder of Kim Proctor, a Canadian high schooler whose burnt remains were found under a bridge.

Two of the victim's supposed friends lured her to their house where they bound, beat, and raped her before dumping the body. A text message sent from the site they disposed of the body served as crucial evidence. Investigators monitored Facebook, including a public memorial page that was set up in her honor, culling potential witnesses there as well as on other public Facebook pages—none of which necessitated a warrant.

Soon, police had enough evidence to secure the necessary judicial authorization to monitor and analyze the suspects' online activities. Keeping them under close surveillance, the police bugged their homes, their cell phones, and even the gazebo where they hung out in the park. Through forensic analysis of the boys' computers and cell phones, they dug up their Google and Wikipedia searches, as well as old transcripts of texts and instant messages. In total, the Tech Crimes Unit amassed the equivalent of 1.4 billion sheets of paper on the two.

The two boys pleaded guilty to first-degree murder and indignity to human remains and were sentenced to life imprisonment with no possibility of parole for 10 years.

craigslist



Get Your Gun on Craigslist!

Mashable.com reports a study conducted by the City of New York found that - despite Craigslist's ban on gun listings - it's quite easy to purchase guns through the online classifieds site. Private investigators found that 82 percent of the time they contacted sellers on Craigslist, an illegal sale was agreed upon.

New York Mayor Michael Bloomberg said the city is now going to crackdown on this practice.

[Forward email](#)



Try it FREE today.

This email was sent to mignolet@bellsouth.net by mignolet@bellsouth.net | [Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Mignolet Business Research Consultants, Inc | 1314 E. Las Olas Blvd., Suite 606 | Fort Lauderdale | FL | 33301