Having trouble viewing this email? www.mignolet.com

CE/CLE Training

Jean Mignolet is proud to offer CLE approved trainings regarding tips for "Locating Hidden Assets" and "Google is not an Investigation" for legal professionals and attorneys. Please contact for available dates.

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 is the top choice of attorneys, corporations, small business owners and individuals who require all types of investigative services.

For further information visit:
www.Mignolet.com

Dear Jean,

With so many new websites emerging daily, it's my job to review those new sources and explain how they are used in today's world of investigation...that is, how to utilize both proven investigative techniques and new technology to get the results you need for your cases.

This coming Saturday, September 5th at 3pm at the Ritz Carlton Hotel in Naples, Florida, I will be giving a presentation to to Business and Computer Section of the Florida Bar.

The presentation is, "Google is not an Investigation," and I hope to see you there!

Jean Mignolet

A reminder that prior issues of the newsletter are viewable from the website.

Smartphones Held Cyber-Hostage with New Ransomware

Ransomware - software that locks your computer until you pay the "ransom" to scammers - it's not just

Contact us at:
Mignolet@Bellsouth.net
or call us at: 954-523-8737 or 954-336-9363

Quick Links

Our Website
Services

Join Our Mailing List!

Craigslist Sex Ad Revenge

Frederick Banks, a 47-year-old from Pittsburgh, PA, has been charged with **posting a fake Craigslist ad inviting men to have come over and have sex with an FBI agent and his wife. The ad included their address and phone number.**

This revenge ad was placed to get back at an FBI agent who had investigated Banks in 2003 on charges of selling unlicensed software.

The suspect alleged the FBI agent had intimidated Banks' girlfriend using a gun, forcing her to implicate Banks, which resulted in his conviction.

Banks is currently awaiting trial for the Craigslist sex ad on

for computers anymore! Cyber-criminals are now using malware to target smartphones, mainly Android products. While the attack on chell phones is relatively new, it has already affected more than a million devices.

Ransomware has been around for years and continues to be a huge problem for PC users especially now that a new "DIY" computer program enables crooks to quickly and easily build their own ransomeware. With everyone carrying their computers around in their pockets and accessing questionable sites and apps more than ever, this is a treacherous time to be a smartphone user.

According to a report from the *New York Times*, some 900,000 users were targeted in just one month with a piece of malware called "ScarePackage." It's easy for an unsuspecting smartphone user to be infected, either via a malicious app disguised as authentic, or by visiting less-than-secure websites such as "adult" sites. The malicious programs are often downloaded from app stores other than the Google Play store, though recently some have even been found there as well.

Ransomware affects your phone by displaying a full-screen message that states it is from the FBI, a government cyber task force, or from a security firm. The message claims that the user has accessed illegal websites and must pay a fine to regain access to the device.

Because these are not legitimate actions by an agency, the payment will be required through untraceable means, like via money wire or a preloaded debit card that the victim provides to the

charges of interstate stalking and harassment.

An ad like this can be placed easily by anyone wishing to harass or intimidate anyone else.

Cybercrime is a relatively new way to victimize strangers, so when attacked, many people are unsure of what to do.

If you are being victimized, go ahead and report the crime, even if you can't identify the culprit. Search online using some variation of the phrase, "reporting cybercrime in [your location]". Remember, law enforcement has access to more resources than you do to search out the culprit.

You may also want to look into what convictions are brought against the culprits of similar crimes. For example, Banks was charged with "interstate stalking." Law enforcement may have

scammers. Whenever you can only pay "fines" using untraceable forms of payment, check out the agency before you lose out to a scam.

In the current boom of cyber crimes, assume that NO APP IS SAFE. There are now thousands of apps available to download to meet any number of needs (and thousands more that seem to serve no purpose at all!). It is impossible for any official App store to police every single app they offer, so ALWAYS use good judgment before downloading an app.

Some tips to avoid getting infected:

* Check an app's trustworthiness on the free www.mobilesecurity.com website.
* Avoid visits to dubious websites.
* Be cautions when using non-Google app stores.
* Change your settings to not allow apps from "Unknown Sources."
* Be wart of new apps that have no user reviews, or apps that only have a very few users.
* Password protect your devices.
* If you have an Android, install security software that can detect malware.
* Schedule regular back-ups of all of your devices.

But if you have already been infected, should you just pay the ransom? NO! Even if you pay the ransom, there is no guarantee that the encryption code to unlock your phone even exists, or that you will receive it. Even if you do manage to get your device back, scammers will still have access to your phone. There are malware programs that can steal information, record calls for blackmail and extortion, send out spam, and wreak havoc with your personal identity.

Your best course of action is to schedule regular back-ups of your device and reinstall the backed-up information to your device. You may also be

trouble identifying which specific crimes have been committed in this new territory of cybercrime, so come prepared with the vocabulary to help get the correct charges to bring your harasser to justice.

able to restart your phone in safe mode and delete the malware. If you are uncomfortable doing this yourself, seek help from a trusted professional.

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