



MIGNOLET
BUSINESS RESEARCH CONSULTANTS, INC.



Investigative Insights...
From
Jean



In This Issue

[Eggs and Abandoned Baby Scams](#)

[Remember 112](#)

[The Worst Passwords](#)

[Hacking QRs](#)

[FaceBook Investigations](#)

[Laptop Tracking Limits](#)



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, corporations, small business owners and individuals requiring

Dear Jean ,

Recently a new member of my private investigators association posted a message expressing concern about having found erroneous information during a background check. I'm certainly glad she did - she potentially avoided facing legal issues. But there was another reason why I appreciated the posting: it was a reminder to me that as a professional I have a responsibility to the client and the subject of a investigation - or I potentially face legal action.

It also underscored the importance of having the resources, skills and knowledge necessary to provide accurate information whether it's regarding a workers compensation claim, employment offer, custody issue, tenant application or someone's life or freedom.

One of the purposes of the state and national associations I belong to is networking and networking is not only about meeting each other and trading referrals, it is also about having colleagues to turn to for guidance and advice. Being negligent in whom we accept as clients, the work we accept, how we conduct our investigations and ultimately what we report is what leads to bad legislation resulting in laws that impact the profession as a whole in the interest of punishing the few who are negligent.

I am a member of the FloridaState Association, FALI, and National Association of Legal Investigators, NALI, the National Council of Investigation and Security Services NCISS, ISPLA, and

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!



Robbers Targeting Stopped Drivers With New Scams

Scam #1

Eggs and Water Don't Mix ... With Your Windshield

Criminals are usually not trained chefs. But some of them know a recipe for robbery.

If you are driving at night and eggs are thrown at your windshield do not stop to check the car, do not operate the wiper and do not spray any water. Eggs mixed with water become milky and block your vision up to 92.5 percent. This would force you to stop beside the road ... and then

on the Executive Council of Legal Aid. Each of these serve a specific purpose for me and our profession.

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

Best Regards,

Jean Mignolet

ALERT**If 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.



The Newest Hacking Frontier: SmartPhone QR Code Scanners

QR codes are riding a wave of popularity. They are also the latest frontier for hackers.

QR codes use an image to hold information that can be scanned by specific readers the same way as a bar code. They've in the past been used for retail inventory, airline boarding passes and event tickets, and direct mailing, but the increased use of mobile devices has made them popular for marketing campaigns and shopping. QR codes placed on billboard and posters around cities allow users to get additional information about a product or company.

"It looks like a gray box with some squares knocked out here and there and you take a photo of that with your phone. It decodes it and sees that it's a URL and takes you to that Web site," said Nicholas Percoco, senior vice president and head of Trustwave SpiderLabs.

become the victim of the criminals who threw the eggs.

Scam #2

Beware of the Baby by the Road

Envision this scenario: you are driving along and see a baby in a car seat sitting by the side of the road. Most of us would stop and rescue the baby.

This is what gangs and criminals want you to do. The location of this car seat is usually beside a wooded or grassy (field) area and the person -- often a woman -- will be dragged into the woods, beaten and raped, and usually left for dead. If it's a man, they're usually beaten and robbed and maybe left for dead, too.

In most instances it's not even a real baby in the car seat.

If you see something like this do not put yourself at risk. Don't slow down. Just dial 911 and immediately notify the police. They will soon pick up the baby (if it is real) or look for the criminals.



It's Not Just 911: Remember 112

One afternoon a woman was driving to visit a friend when an

The problem is that some QR codes are taking people to bad websites with malware, spyware and other malicious code. Hackers can then remotely access all of the data in a person's phone and record their every move through pictures and audio, according to cybersecurity researchers. And there's no way to know once a device is infected.

According to an article on securitymanagement.com, Kaspersky Lab discovered the first instances of QR code tampering in September. A Russian app called Jimm that contained a virus that sent text messages to a premium rate number, comparable to calling a 900-number in the U.S., was being downloaded through a QR code by smartphone users in Europe. Text messages to the service cost six dollars per message.

By early October Kaspersky had detected QR codes linked to malware for Android and J2ME - the cybercriminals' favorite mobile platforms, according to Kaspersky's September malware report.

"When users are affected with malware on a mobile device, there's little visibility in the security world of what that looks like. Most security software is looking for malicious apps, but not something from a malware standpoint," Percoco said.

Percoco says hackers could build a rouge QR code in a matter of minutes and deploy them as random stickers or overlays on existing QR codes. Many legit QR codes are displayed in public, with no explanation to entice customers into decoding the image to see what's next.

"There was a billboard that was 30 feet by 15 feet in downtown Chicago that was literally only a QR code," Percoco said.

The protection against QR code-based attacks, Percoco said, is not to "scan random QR codes you see while walking on the street." The second is to use a QR app that doesn't send a browser directly to a Web page. Some apps show a preview of the Web page or the URL that the code directs to.

"There aren't a lot of mechanisms, from a mobile perspective, to look for malicious sites. **So that being the case, the best solution is to avoid QR codes where you can or if you don't trust the source,**" he

unmarked car pulled up behind her and put his lights on. The woman's parents always told her never to pull over on the side of the road for an unmarked car, but rather to wait until they get to a gas station, etc.

The woman had actually listened to her parents advice, and promptly called 112 on her cell phone to tell the police dispatcher that she would not pull over right away. She proceeded to tell the dispatcher that there was an unmarked police car with a flashing red light on his rooftop behind her. The dispatcher checked to see if there were police cars where she was and there weren't, and he told her to keep driving, remain calm and that he had back up already on the way.

Ten minutes later 4 cop cars surrounded her and the unmarked car behind her. One policeman went to her side and the others surrounded the car behind. They pulled the guy from the car and tackled him to the ground. The man was a convicted rapist and wanted for other crimes.

The 112 Cell Phone feature is not well known. It is actually a link to state trooper information and works in all 50 states. Further, women alone in a car should not pull over for an unmarked car. Apparently police have to respect your right to keep going to a safe place.



25 Worst Passwords Of 2011

Pro tip: choosing "password" as your online password is not a good idea. In fact, unless you're hoping to be an easy target for hackers, it's the worst password you can possibly choose.

"Password" ranks first on password

said.

facebook

Social Sleuths

Information from FaceBook and other sites now researched by Private Investigators

The telephoto lens is still one of a private investigator's most valuable tools, but a Facebook account is becoming just as important.

Especially in the business world.

The Cleveland Plain Dealer recently reported on the increasing trend of corporations hiring private investigators to trawl social-media sites for intelligence about competitors and to watch for insider leaks, product complaints and evidence of employee misconduct.

The article explained that investigators still use the old-fashioned ways -- snapping secret photos, slapping global positioning devices onto cars and tunneling through criminal files. However, today's corporate sleuths spend more time mining the mass of information people put online about themselves.

"We use social media primarily to research people", said Avon Lake native Kristin Wenske, an investigative analyst in New York City with Corporate Resolutions Inc., an intelligence service. Wenske's clients are mostly private-equity firms and hedge funds, and before they plow hundreds of thousands or millions of dollars into a company, they want to make sure its management team is clean.

Private investigator Tom Pavlish of Cleveland also has been assigned to check into chief executives of companies targeted for acquisition. In one case, the CEO had a favorable public image, but research unearthed sexual harassment accusations from two sources. Pavlish's client decided not to keep the executive when the deal closed because of the potential exposure and liability if the

management application provider SplashData's annual list of worst Internet passwords, which are ordered by how common they are. "Passw0rd," with a numeral zero, isn't much smarter, ranking 18th on the list.

The list is somewhat predictable: Sequences of adjacent numbers or letters on the keyboard, such as "qwerty" and "123456," and popular names, such as "ashley" and "michael," all are common choices. Other common choices, such as "monkey" and "shadow," are harder to explain.

As some websites have begun to require passwords to include both numbers and letters, it makes sense varied choices, such as abc123 and trustno1 are popular choices.

SplashData created the rankings based on millions of stolen passwords posted online by hackers. Here is the complete list:

- 1. password
- 2. 123456
- 3.12345678
- 4. qwerty
- 5. abc123
- 6. monkey
- 7. 1234567
- 8. letmein
- 9. trustno1
- 10. dragon
- 11. baseball
- 12. 111111
- 13. iloveyou
- 14. master
- 15. sunshine
- 16. ashley
- 17. bailey
- 18. passw0rd
- 19. shadow
- 20. 123123
- 21. 654321
- 22. superman
- 23. qazwsx
- 24. michael
- 25. football

manager repeated his conduct.

"Remarkably, I've developed negative information even from LinkedIn references," Pavlish said.



Laptop Tracking Company can be Sued For Spying on Sex Chats

A columnist at CNET.com recently wondered whether online or off could someone be watching you. He then raised the question if there is a limit in what they're allowed to see?

In a recent case in Ohio a judge decided that it might not be permissible for a laptop-tracking company to espy some of the more intimate parts of your life and body--even if they are being displayed on a stolen laptop.

A Wired report suggests that Absolute Software was quite wired into where an allegedly stolen laptop might be. However, it might not have been within its rights to capture intimately revealing images of schoolteacher Susan Jeffrey, who was in possession of the laptop at the time.

Jeffrey says she bought the laptop from one of her students in 2008. However, it actually belonged to the Clark County Schools District in Ohio. It had allegedly been stolen by a student, then sold to another student, before being resold (for \$60) to Jeffrey.

The school district hired Absolute Software, whose range of fine services included LoJack whose motto is: "We get stolen laptops back."

U.S. District Judge Walter Rice opined that it was important to know how LoJack gets stolen laptops back.

"It is one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it

SplashData CEO Morgan Slain urges businesses and consumers using any password on the list to change them immediately.

"Hackers can easily break into many accounts just by repeatedly trying common passwords," Slain says. "Even though people are encouraged to select secure, strong passwords, many people continue to choose weak, easy-to-guess ones, placing themselves at risk from fraud and identity theft."

The company provided some tips for choosing secure passwords in a statement:

- 1. Vary different types of characters in your passwords; include numbers, letters and special characters when possible.
- 2. Choose passwords of eight characters or more. Separate short words with spaces or underscores.
- 3. Don't use the same password and username combination for multiple websites. Use an online password manager to keep track of your different accounts.

down but it is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop," his decision reads.

The accusation here is that Absolute didn't merely report the IP address to the police. It also allegedly got its eyes on e-mail and other chats between Jeffrey, 52, and a paramour. Some of these interceptions allegedly included nude pictures of Jeffrey.

In its defense, Absolute said that Jeffrey should have known that any laptop bought for \$60 must have been stolen.

In his ruling, the judge decided that Absolute might employ fine and upstanding people, but that "a reasonable jury could find that they crossed an impermissible boundary."

This case may remind some of the Philadelphia school district which last year was accused of Webcam spying on one of its 15-year-old students while he was in his bedroom. The case concluded late last year with a payment being made of \$610,000.