MIGNOLET
BUSINESS RESEARCH CONSULTANTS, INC.

CE/CLE Training

Jean Mignolet is proud to offer state 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

Dear Jean,
Students and small business owners are some of the busiest and most strapped-for-cash folks out there. Between their huge workloads and steep learning curves, they have to juggle a ton of different tasks and responsibilities every day. Did I mention they're strapped for cash? This all makes students and small business owners prime targets for financial scams.

Protect yourself. Take time to think through decisions about offers that sound too good to be true and investigate exactly who you are dealing with. This is a learning curve you DON'T want to climb the hard way.

Jean Mignolet

A reminder that prior issues of the newsletter are view-able from the website.

Know Your Predator:
Be Aware of the Scams that Target YOU

Small Business Owners: The Devil's in the Details

visit: www.Mignolet.com

Contact us at:
investigators@Mignolet.com
or call us at: 954-523-8737

Quick Links

Our Website

Services

Join Our Mailing List!

Mobile Phone App Makes Breaking In Easy!

The mobile phone app KeyMe is a key management app that enables you to keep a digital copy of your physical key stored in the Cloud by scanning an image of it with your phone. You simply scan your key, which creates a digital version of the imprint, and bring it to a hardware store or self-service kiosk to make a physical copy from the digital copy on your app.

This app was designed for people who accidentally lock themselves out of their houses-with their phones, of course. Unfortunately, it also allows ANYONE with the KeyMe app scan ANY key with their mobile phone and make a physical, working duplicate copy. You can see where this is

You're busy, you're multitasking beyond all reason, and you're dealing with steep learning curves as your business grows and evolves. Scammers are WELL AWARE of this and will try to take advantage of you.

When your business begins to accept credit cards, there are several scams to look out for. The first is to be on the lookout for FAKE PROCESSING SERVICES. When you're looking for a credit card processing service, check in with your bank before you agree to anything with anyone. Small businesses get bombarded with calls from representatives from processing service companies, and some of these companies are fraudulent. Once they sign you up they will either charge very high fees or just take your money.

If you have a card-swiping device through your Point of Sale (POS) system, you may receive bogus calls that purport to be from your card processing company or your POS system supplier saying they need to install updates or modifications to your equipment. If this happens, check in with your company directly to make sure this call is valid because these upgrades or modifications may actually be hijacking your hardware to capture card numbers.

Another financial scam that targets small business owners also preys on busy schedules. Scammers will call the business posing as the utilities company or the liquor board demanding payment NOW on a past-due bill. These are designed to make you respond to urgency and pay a bill that simply does not exist, giving the scammer your credit card or checking account number in the process. It is important that you NEVER respond to these calls. You can protect yourself simply by understanding that REAL past-due payment requests come by MAIL and not by phone.

All of these scams that target small business owners bank on the chance that you will not have the time to investigate and verify who you are dealing with. When it comes to dealing with your money and the money of

going.

KeyMe claims that there are built-in security features to this app to protect against people who may want to break into your house or steal your car from using pictures they get of your keys from making them into physical copies that will actually work to open the door to your house or start the ignition of your car. Unfortunately, when put to the *real world test*, these security features fall dangerously short.

KeyMe requires you to use email, fingerprint, and credit card verification when making physical copies from digital versions of keys photographed with KeyMe. Also, whenever there is activity on this app, an email notification will be sent. However, this is only useful if YOU have KeyMe on your phone and your phone has been stolen and someone is trying to use YOUR phone to make a key to break into your house or steal your car. Someone else with a KeyMe app who takes a picture of your key with their phone simply has to verify THEIR email, fingerprint, and credit card to get a physical copy made of YOUR key.

Here is another unfortunate

others, take the time and steps necessary to know ALL the details.

***

College students: Fake Checks and Debit Card Scams

You're working hard, you've got little time for a job on the side, and you need money. This makes you vulnerable to scammers offering you fast and easy cash, be it through an ambiguous part-time job that seems to good to be true, or by luring you into selling your bank and debit card information. Here are some common financial scams that target college students to look out for.

This first scam is a variation of a well-known scam particularly tailored to target college students. What ultimately happens is the student gets a check in the mail and must wire most of it to a third party. The ruse is that the student is hired for an ambiguous telecommute administrative assistant job that pays $300 per week. Their first task is to cash a check for $2,000 that they will receive in the mail and wire all but their $300 to a third party recipient. Of course, the check will bounce, the student will be left with the debt, and the scammers will make out with $1,700.

A related version of this scam happens when students are asked, usually via social media, to let someone use their bank account to process a check. The student is told they get to keep half of the money. Sometimes scammers even fabricate an excuse to get the student to give them their debit card PIN number. The scammer deposits a counterfeit check in the student's account and then collects most of it. When the bank discovers the check is counterfeit, the student is left with the consequences.

Another financial scam takes place at nightclubs and other places students frequent to party. In this con, students are lured into selling their debit card numbers and PINs. In this case, the scammer will deposit a fake check into their account and withdraw the amount in its entirety. Then, the student can call in and report his card stolen so he will

security glitch: The makers of KeyMe claim the app will only generate a workable copy if the key is removed from its chain, placed on white paper, and photographed on each side from four inches away. However, this security feature ALSO failed the *real world test*. Casual photographs taken of keys attached to their rings have turned out workable copies.

A spooky aspect of criminals using KeyMe as a means of breaking and entering or auto theft is that victims will be left in the dark as to how the deed was done. Most people do NOT know about KeyMe or suspect that it would be a tool used by the culprit to break into their homes.

What can you do to protect yourself, your keys, and your home? The most effective thing you can do is to keep your keys in your purse or your pocket and not leave them lying around anywhere. Also, be wary of valet parking.

not have to suffer the consequences. This is of course illegal and if the conspiracy gets uncovered the student could face serious charges.

While this all sounds incredibly sketchy right off the bat, the prospect of making some quick money when you're busy, paying high tuition fees, on a tight budget, and out on your own for the first time, it's easy to fall prey to scammers making offers that sound too good to be true.

::