Kiamalu Consulting & Investigations LLC

Serving All The Islands Of Hawaii And Worldwide

SPECIAL EDITION

THE KIAMALU REPORT

VOLUME 3, ISSUE 1 APRIL 2016

Welcome to this special issue of the Kiamalu Report.
In this issue we will discuss Cyber Crime Scams and why hiring a private investigator can substantially help your case.

**The internet is like a double edged sword which can be used for both positive and negative purposes.**

Today the Internet is one of the most important parts of our daily life. You could say that with the progress of the internet we are progressing in *every* sphere of life, and it not only makes our tasks easier, but also saves us a lot of time.

Internet availability is not limited to desktops or laptops anymore. Our world is filled with tablets, iPads, watches, mobile phones and other devices all with internet functionality, readily available and affordable.

By contrast, television took more than 25 years to reach 10 million users, whereas computers took over 10 years to reach the same number.

The ***internet***, however took less than *5 years* to reach the same number.

Recent studies show that even in the developing countries like India more than 40% of people are using the internet and the purposes of internet usage is diverse.

By far the easiest thing that can be done using the internet is that we can communicate with people living far away with extreme ease and i*n Real Time.*

Research on anything or ***any person is uncomplicated and very simple.*** And with the added aspect that people can spend unlimited amounts of time tracking down anyone. To collect information and reach someone is very easy, to the point that a new type of crime is quickly emerging .....

Continued Next Page

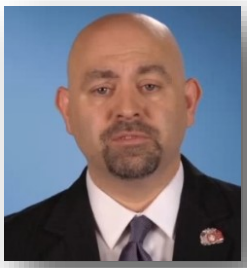

**KCI IS A U.S VETERAN OWNED & RUN COMPANY**

**SPECIALIZING IN THE UNIFORM CODE OF MILITARY JUSTICE (UCMJ)**

***SEMPER FI !***

**INSIDE THIS ISSUE:**





***Nathan Moores***
***Director of Operations***
***CEO***

**If you have questions about any of our services or need our assistance please feel free to contact us.**

***Our highly experienced investigators are skilled in all types of investigations and intelligence gathering.***

Here is a recent case we painstakingly pursued to a satisfying conclusion:

"Our client was a Naval officer who was receiving threats from someone online claiming they were a family member of a minor he allegedly solicited for sex. There was no merit to the allegations. After receiving this threat, he and individuals close to him were continually threatened with legal action and other physical harm in an elaborate international scheme to extort money from him.

Kiamalu Investigations, with coordination and legal advice from Bilecki & Tipon LLLC, took extensive steps to track the source of the scammers, exposed them and stopped the harassment, threats and extortion.

We also worked with the NCIS office in charge of these particular cyber security threats to ensure that the extortion attempts stopped and that the NCIS case against our client was closed."

**There are many levels of security clearances in our Armed Forces. All of those individuals may be susceptible to some kind of extortion attempt from extremely clever scammers bent on stealing classified secrets and threatening our National Security. Kiamalu Investigations will continue in our efforts to thwart these extortion scammers and help secure our Nations vital information.**

**Kiamalu-ci.us | (808) 664-3260 | Century Square Building, 1188 Bishop Street, Suite 1812, Honolulu, HI 96813**

## The Internet Is Like A Double Edged Sword cont.

### Cyber-Crime

Any crime that is committed over the Internet is referred to as a **cyber-crime**. There are many types of cyber-crimes and here are most common ones:

- **Hacking:** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

- **Theft:** This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber-crime and there are laws that prevent people from illegal downloading.

- **Malicious Software:** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

- **Child soliciting and Abuse:** This is also a type of cyber-crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

- **Cyber Stalking:** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

- **Identity Theft:** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber-crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history. This type can and often does turn into *Blackmail*.

### Causes of Cyber Crime

Wherever the rate of return on investment is high and the risk is low, you are bound to find people willing to take advantage of the situation. This is exactly what happens in cyber-crime. Accessing sensitive information and data and using it means a rich harvest of returns and catching such criminals is difficult. Hence, this has led to a rise in cyber-crime across the world.

***While*** everyone with a Computor is vulnerable, ***Military Personnel and Veterans*** are often frequently targeted for some special **Scams** because of their specific situation.
**Here are some of those Scams:**

Continued Next Page .....

### In The News
### Top Scams for 2016

**#1. Tech Support Scams**
**Reported countries:** India and Pakistan
**Damage report:**
**$100 to $1000 to fix problem.**
In many cases, scammers used U.S. VOIP phone numbers.
Scammer call victims and tell them their computer has become infected/bugged. Take control of computer to fix.

**#2. Fake/Counterfeit Merchandise Scams**
**Reported countries:** China
**Damages report:** $100-$1000.
Scammers usually ask for payment via credit card. Victims have also reported identity theft at a later time.

**#3.Online Dating Shaming and Blackmail**
**Reported countries:** African, India, Pakistan
**Damages reported:** $500 - $3000+
Victims are threatened with exposer of an embarrassing sexual relationship. The relationship may or may not be true. The threat may be with legal action and or physical harm in an elaborate international scheme to extort him for money.

**#4. Payday Loan Scams**
**Reported countries:** India, Pakistan
**Damages reported:** $500 - $3000+
Scammers pick their victims from those most in need -- people who are willing to take out high-interest payday loans. They ask for upfront money then never follow through with any sort of loans.

## Scams That Frequently Target Military Personnel and Veterans

- **Protest Scams:** Not every online military scam is created for financial gain. Some scammers are contacting the families of military members by phone or email and making false claims that their son or daughter is injured or wounded overseas. They sometimes ask for money for medical bills, but usually they are only contacting the family to scare them as an anti-war protest.

- **Craigslist Car Scam:** Scammers are taking to Craigslist, offering too-good-to-be-true discounts on cars for military personnel. In some cases, the scammers claim they are *military members* about to be deployed and need to sell a vehicle fast. Similarly, others offer *military members* a *special discount* for serving their country. More disturbingly, the scammers are offering low-priced vehicles because a *U.S. military member who died in combat owned the vehicle and the family wants to get rid of it fast.* The Better Business Bureau (BBB) says scams like these usually require a wire transfer and promise free shipping. The description of the cars is lifted from auto sites, and typically you can Google the vehicle ID number, to determine whether it's a real deal or a hoax.

- **Housing Scams:** Due to the nature of military service, those who serve and their families are forced to move from base to base around the country. Though the military often provides housing, some members are responsible for finding their own living arrangements, which scammers are fully aware of. Scammers go to Craigslist to target areas where they know military members will need housing. They lift the descriptions of legitimate rental properties and rewrite the post so it offers a special discount for military members. Depicting a too-good-to-be-true offer, they ask for a security deposit to be wired in advance to ensure their occupancy. But often, the individual or family arrives at the rental property only to find it already occupied.

- **Online Dating Scams:** These are the latest and most popular to hit the web. Scammers, usually out of Ghana or Nigeria steal identities of real soldiers on social networking sites like Facebook and Myspace and pose as military members. After posting pictures and stories to popular dating sites, the scammers contact women. "They build up a huge elaborate story about who they are, they are heroes and serving the country. People fall for this ploy, and some people are sending them money. Scammers ask for everything from laptop computers to money for airfare so they can fly back to the U.S. and visit the victims, most of whom are women. They are very poetic, they are very savvy. Luring these women in and they take them for their money. Victims have been cheated out of thousands of dollars. And in some cases women have taken second mortgages on their homes to finance romantic interest overseas.

- **Blackmail Scams:** Some romance scammers seek out a niche of various fetishes where they will find an obscure fetish and they will make the victim think that if they pay for the scammer's plane ticket that they will get to live out a sexual fantasy of theirs by having the scammer come to them to have sex. The scammers also like to entice victims to perform sexual acts on webcams. They then record their victims, play back the recorded images or videos to them and then extort money to prevent them from sending the recordings to friends, family, employers, often discovered via social media sites such as Facebook, Twitter etc. This type of scam can affect your social standing amongst family, friends and your work. *What will people think about you?* After all blackmail is a crime that does require the victim to participate by giving someone the information and or tools to hurt them.

*Recent trends show that publicizing the personal life and information of an individual on social network websites is increasing and the tendency of considering the virtual online world as real world is increasing very rapidly.*

### *Cyber Criminals Work Together*

It has been shown that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control.

Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals.

While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task.

This is primarily because of the methods used by cyber criminals and technology keeps changing too quickly for *law enforcement agencies to be effective*.

That is why commercial institutions and government organizations need to look at other methods of safeguarding themselves.

## Tips to Protect yourself and your family

**While federal agencies are committed to using all of their tools to hold these scam artists responsible, the best way to fight them is to deprive them of customers. Here are a few tips on how to protect yourself and your family:**

- **Be wary of up-front fees:** Scammers often say that they can help you access your benefits or get a good interest rate on a loan if you provide them an upfront fee.

- **Always find out what the total price is:** Scammers hide the true cost of a product through numerous installment payments. They can offer misleading information about how much something really costs once all the payments and fees are added up. If the total price is too high, take your business elsewhere.

- **Don't trust promises about the future:** Some scammers will promise changes to the terms of the loan that will occur in the future. Before handing over any money, make sure that everyone agrees to the final terms of a deal.

- **Find out with whom you are dealing:** Some scam artists will portray themselves as something they are not in order to get your business. They'll say something like, "I'm a veteran of the armed forces," to try to gain your trust. If you are worried about validity of the salesperson, ask your installation community service office about the company or individual. You can also contact the Better Business Bureau.

- **Be wary of house calls and telemarketers:** If an individual comes to your door or calls your house promising assistance with accessing your Department of Veterans Affairs benefits, you should be wary of the validity of their service. The VA doesn't generally make house calls, and it doesn't participate in telemarketing. These scammers are not at your door to provide a public service or reward you for your military service. They want your personal information and access to your financial accounts.

## What A Private Investigator Can Do For You

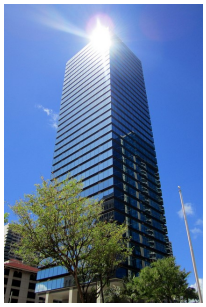
At *KIAMALU* we are ready and able to help protect you.
Our highly experienced investigators are skilled in all types of investigations and intelligence gathering.

Our solution to these type of problems allows us to use a system of seamless sharing and access of information within a specific security classification that cannot be intercepted by or advertently revealed to a user who is not part of the security classification. This helps to keep the network and the systems using the network safe.

*Our device forensic services include,*

*Cell Phone Data Recovery from over 10,000 models of mobile phones (Apple, Samsung, Blackberry, LG and More!)
*Mobile Phone Spyware Discovery (yes, a cell phone can be bugged!) *Consulting/Case Analysis *Incident Response

**FOR ADDED INFORMATION CHECK OUT OUR NEWSLETTER ON:**
**CELLULAR PHONE FORENSIC EXAMS**



***In today's economic climate Kiamalu Consulting & Investigations realizes how important it is to get the most from your budget, without sacrificing on the quality of the services you need. With Kiamalu you can rest assured that we take pride in our work and because of our high skill level and extensive experience, we are able to offer services that are customized to your budget and your needs, resulting in a successful relationship.***

**Contact Kiamalu Consulting & Investigations to discuss the facts and circumstances of your particular case with an experienced investigator.**
Kiamalu Consulting & Investigations LLC offers free initial 30-minute consultations. However, no advice beyond that initial consultation can be provided without a signed engagement letter and payment of KCI fees. Please call our offices or visit us online at: Kiamalu-ci.us

**(808) 664-3260**