

CRIME FIGHTER

The Safety Newsletter of the Oro Valley Police Department

Fourth Quarter 2014

Inside This Issue

How is Identity Theft Happening Today?.. 2

Suspicious Activities - Drug Houses 4

Understanding the Crime Triangle 5

Halloween Safety Tips 6

Contact Information 8

Face Stalking



Facestalking – A play on the term “stalking” and a common method of cyber stalking using “Facebook.”

What is it?

As with all things in our society, technology is revolutionizing the way crime occurs in facets that are happening so fast, we can't even recognize them as they happen.

One of those safety concerns that's being transformed is stalking. Stalking traditionally has meant knowing the person you're targeting, be it a former lover, etc., and proceeding to follow them around. This obviously requires a great deal of time and resources to be able to dedicate to the prey, and the predator is usually known to the victim. Famous examples of stalkers include John Hinckley who fixated on Jodie Foster in the late 1970's. He even went so far as to pay visits to her dorm room while she was in college and making disturbing phone calls to her. Fortunately for investigators, Hinckley recorded the phone calls and the evidence was easily obtained. The audio from these phone calls also offer a realistic glimpse at the terror the victim can endure (Jodie Foster can be heard pleading with him to stop contacting her) and just the sheer creepiness of stalkers.

Advance to today and we find several interesting changes in the way stalking continues in the digital age. Keep in mind, stalking, much like other crimes, doesn't get eliminated with the advent of new technologies. It becomes enhanced and complicated, creating new avenues for predators to attack, and making the investigators' task even more complex. We also find the face of the stalker changes significantly with the advent of cyber stalking.

Traditional stalking saw about 70% of the stalkers being male. Today, males make up about 40% of the victims in cyber stalking cases. The most common example one can think of is the jealous ex-lover who uses various social media sites to keep tabs on their former affections. Once a new challenger is located, the jealous ex can use the social media avenue to begin harassing the victim(s).

Other issues arise when couples split and they shared social media accounts, or other things like email addresses. Once that ex has your password, they can also do a significant amount of damage to your life, contacting friends, coworkers, or family, and masquerading as you.

The dollar amount on this isn't cheap either. One study found that the average cost of traditional stalking was about \$500. The costs associated with modern cyber stalking go up significantly and average around \$1200. Things like changing phone numbers, moving, and even changing one's name can get very expensive very quickly.



www.ovpd.org

Facestalking Continued

Tips to protect yourself:

- Don't become involved with people who have a history of this behavior. If it happened before, chances are it will continue to occur. Never try to rationalize away behavior that is dangerous.
- Never share your passwords. Compromised passwords continue to be one of the primary routes cyber crime, in all forms, occurs.
- Make sure your profiles are set to "private" or "friends only." If a former acquaintance is behaving in this manner, limit their attack vectors by removing them from your connections in social media.
- Check with your friends to see if they are still friends with the stalker. Many times, an attacker can gain significant information by still being connected with your friends. You may want to talk to your friends about what their accounts permit the ex to see.
- If you do change your phone number, don't have your name on the new voicemail greeting. Perhaps leave the voicemail set-up as a generic computer voice simply repeating the number. A great deal of information can be gleaned off of voicemails.

If you're wondering if this is illegal the answer is: Yes, it is!

Arizona Revised Statutes Title 13-2916 says the following:

"A. It is unlawful for any person, with intent to terrify, intimidate, threaten or harass a specific person or persons, to do any of the following: . . . 3. Otherwise disturb by repeated anonymous, unwanted or unsolicited electronic communications the peace, quiet or right of privacy of the person at the place where the communications were received."

So, don't do it! It's illegal, unethical, and flat out wrong.

Not to mention really creepy. . .

How is Identity Theft Happening Today?



In the modern age of inter-connectedness at a level never before seen by humans, we're seeing crimes happen on a scale that's unprecedented. The surging crime of our day is fraud and its cousin, identity theft.

First, let's define the two because while they're similar, there's also some differences.

Fraud is defined as "the crime of using dishonest methods to take something valuable from another person" (Merriam-Webster.com). Fraud can be a very general term that is assigned to a multitude of different crimes. Examples of these include social engineering scams, fake contests, and the usual "you won something for nothing" lie.

Merriam-Webster defines identity theft as "the illegal use of someone else's personal information (as a Social Security number) especially in order to obtain money or credit". Many times, some sort of fraud may be used to help identity theft occur. Some of the more common examples of this include duping users in to handing over their passwords to a criminal actor in order for them to log in to your banking account and take money. Of course, some one lying and using a stolen identity to fraudulently obtain a credit card is a fraud, and identity theft.

How is Identity Theft Happening Today? Continued

HOW IT WORKS

This is where the hackers come in to play. Let's say you're looking for names, DOB's, social security numbers – you know, the kind of stuff you'd need to start opening fake checking accounts. The hackers would go to where this information is located and obtain it somehow. In some cases, it's as easy as searching for the right terms on google and finding a poorly designed website or database that's easily accessible. This method is called "google hacking." In other cases, it could be stealing a laptop that has personal information stored on it (a 2006 theft compromised the identities of 26.5 million veterans after a VA official had his laptop stolen).

Once the personal information is available, you can go to underground criminal websites that trade and sell stolen identities and credit card numbers. These are called "Carding forums" and a google search will instantly return search results for dangerous websites that you should probably never visit. Now that you know, NEVER go to those websites! Another search term is "fullz." This will return full SSN, DOB, names, etc., and this information is how a number of frauds occur.

Think of everything you use that information for. Filing your taxes, getting your tax return, opening new credit cards, making purchases on-line, and so on. All that criminal has to do in order to start being you is go to this website and find that information.

But how prevalent is the information out there? Who has been exposed? Is there any way to keep your data from falling in to the wrong hands?

Sadly, this information is practically ubiquitous. In late 2013 it was learned that Experian, one of the three credit reporting organizations, had been duped in to selling consumer info to one of these ID theft websites. (For more reading, check out Brian Krebs' article on the subject here.) Furthermore, many celebrities (Michelle Obama, Beyonce, Paris Hilton, etc...) had their personal information posted on some underground websites that detailed their name, DOB, SSN, and even their credit card numbers.

Now if these criminals are able to go out and get that kind of information on politicians and celebrities, what's keeping them from getting the information of the average citizen?

Furthermore, in 2013 alone, there were approximately 2,164 **reported** data breach incidents, that exposed somewhere around 822 million records. (Who says they all get reported?) One breach alone at Adobe compromised 152 million names. The simple fact of the matter is, until organizations that have our data start taking better care of it, no one is safe from identity theft.

WHAT CAN WE DO?

As individuals, we need to be monitoring our credit reports, our checking accounts, and all of our financial statements. A keen eye for suspicious activity early on will help limit our exposure and damage to these kinds of incidents. The reality is, we can't expect our banks or our credit card companies to be guarding all of this for us – there's simply too much of it going on to expect them to play credit card nanny and catch all of it. That's why it's incumbent on us that we take our financial security seriously, and personally.

Furthermore, there are methods you can use to protect yourself, like using your credit card instead of your debit card as much as possible. A fraudulent charge on a credit card can be disputed, and there's a lot more protections in place for consumers when making credit purchases rather than using debit cards. For now, at least.

And finally, get involved. Reach out to your elected representatives on policy issues surrounding these issues, and demand higher levels of protection for yourself, and your finances.

Suspicious Activities – Drug Houses

In this month's edition we'll talk about houses that may indicate narcotics activity that ought to be reported to police.

It's no secret that Tucson has a drug problem. Some estimates say Tucson sees about 70% of the narcotics traveling from South America in to the United States, and Tucson is an integral regional hub in the narcotics trafficking network. A common question is, What kind of activity would seem suspicious? I'll give you an example of behaviors that I observed as a child.

We had some neighbors who would keep to themselves (quite common today, sadly), but to an extreme not commonly witnessed. Whenever we would see them, they would be outside only very briefly. The bigger issue was the hours they kept. The house would be very quiet, almost vacant, for days or weeks at a time. Suddenly, a flurry of activity would erupt – sometimes 4 cars would be there. Then there would be people working around the clock in the house. Vehicles (mainly pickup trucks) would back in to the garage, and the garage would be open for only long enough to get a vehicle in and out – never a moment longer. There would be activity in the middle of the night until suddenly, everyone hopped in their cars and drove away at 3 AM in the morning.

One day I was walking to the mailbox when over a dozen unmarked police cars pulled up and a bunch of officers from the "task force" hopped out. All very exciting for a 14 year old who watched too much TV, but not very comforting for my parents. We found out that our "neighbors" had actually been drug traffickers. What could have been the biggest drug bust of my career was mere feet from where I played in the backyard...

Unfortunately, we just didn't know. While we did think it odd, it never crossed our minds that these people would be international narcotics traffickers. We just didn't think that way. That led us to get involved with our neighbors going forward. Fortunately, the cartels have known better than to park their cars next door since then.

This story is a perfect example of why it pays huge dividends to have neighbors being neighborly, something that gets more and more difficult in our busy world. A few things that might seem suspicious are things that neighbors, as well as owners of rental properties, should be aware of:

- Odd hours/strange hours. Human beings are not nocturnal animals. Criminals tend to be, however. With that said, if you notice unusual activity at unusual hours, it should be considered unusual. Kind of obvious, but trust your instincts on this.
- No furniture. People tend to live in houses with things. They have things like couches, chairs, and the other various trappings of living. A standard drug transfer house will have maybe a few chairs, and blow-up mattresses. It looks more like people are camping out there, which is basically what is happening.
- You notice odd trash. Things like tons (sometimes literal tons) of saran wrap, plastic wrap, or brown paper piling up could indicate narcotics activity. Fortunately, meth labs are extremely rare in neighborhoods these days. That's because the drugs are produced elsewhere in mass quantities, but they're still transferred to residences where they can be taken out of their initial bulk packaging and repackaged in to smaller sizes for mid-level or street-level sales.
- The windows never open. This could be for several reasons, but if the shades are always closed, that might be because they're trying to hide what's going on in the living room.
- Remodeling the house/car at 2 AM. If you hear what sounds like a wall being cut down in the middle of the night, that's not normal. It's common to see the house ripped apart to accommodate a more efficient drug factory. Combine remodeling with typical drug user Time Zone, and it will sound like there's construction going on at very odd hours.

So, what do you do if you think you live next door to Walter White? Call 911!

There's additional resources your police department will utilize, and it may be wiser for law enforcement to sit and watch the house to monitor the suspicious activity and gather additional information. Don't be disappointed if it seems like the activity isn't addressed immediately – it's very likely it's being investigated in a manner that you can't see.

Understanding the Crime Triangle

The crime triangle is an idea that there are three elements necessary for a crime to take place: Opportunity, motivation, and ability.

Motivation is the desire or reason why the crime is taking place. An example of this might be the financially motivated criminals who need money for various reasons. Whether it's the need to pay for an expensive drug habit, or living beyond their means, the motivation is up to the criminal actor themselves. In some cases incentives for doing the right thing can motivate the criminal to not conduct the criminal activity. Most commonly, we use prison or incarceration as a deterrent to conducting the criminal activity.

The next aspect is ability. Does the criminal have the capability of committing the crime? In Arizona, it's against the law to even possess tools used for burglary. By keeping the tools used for crimes out of the criminals' hands, we try to lessen the ability for crime to occur. Another example is gun laws and forbidding convicted felons from possessing firearms.

As you might guess, these first two factors aren't something we can control very well. As a society we try, but overall, it can have spotty success. Ultimately, a dedicated criminal will not adhere to the laws that forbid possessing burglary tools, and will still have the motivation to commit the crime.

Finally, the opportunity to commit the crime is the factor we can control the most. An example of this might be the store that locks up high-priced items that are stolen frequently. By making it more difficult to commit the crime, you can impact the crime.

So what things can we do that make it more difficult to commit a crime?

Target hardening speaks directly to this. An extreme example is a nuclear missile silo. Lock yourself underground in a giant concrete bunker with armed security teams patrolling (with machine guns) the hatch and give no one the keys. More realistically is doing simple things around your home like making sure your home is well lit to the front, and locking your doors on your home and vehicles.

Sadly, the department recently had a rash of reports where vehicles had items stolen out of them. The vast majority of these cases involved cars that weren't even locked.

Another easily accomplished method is to not leave high-risk items in easily accessed places. Things like personal electronic devices, laptops, and financial documents should never be left in a vehicle sitting out in the open – be it in your driveway, or a parking lot. These items are protected by mere millimeters of glass which breaks easily with the Arizona Master Key – a large rock found nearby. As you can see, it's very to see how quickly your valuables become someone else's.

A crime can only occur when all 3 of those elements are lined up correctly. The best way to protect yourself is to maximize and properly influence what you have control over. So do your part and make it harder for bad guys to do their job!

Halloween Safety Tips



Everyone wants to have a safe and happy Halloween for themselves, their children and their guests. The following safety tips can help you make the most of your Halloween:

- Your children should wear costumes with reflective markings, and bright colors.
 - Costumes should not drag on the ground.
 - Make sure children are wearing flame retardant costumes.
 - Plan your trick-or-treat route ahead of time and make sure your family knows it.
- Never allow small children to trick-or-treat without an adult's supervision.
 - Only visit houses that have their lights on.
 - Walk on sidewalks.
 - If there is no sidewalk, walk with the road on your right side.
 - Cross the street at the corner or in a crosswalk.
 - Take a cellular phone with you if possible.
 - Carry a flashlight.
 - Tell your children to only accept treats in the doorway and never go inside a house.
 - Tell your children to allow you to go through their candy before they start to eat it.

Halloween Candle Safety Tips

In general, candles are fairly safe products, but may become hazardous when used improperly or used in an unsafe manner.

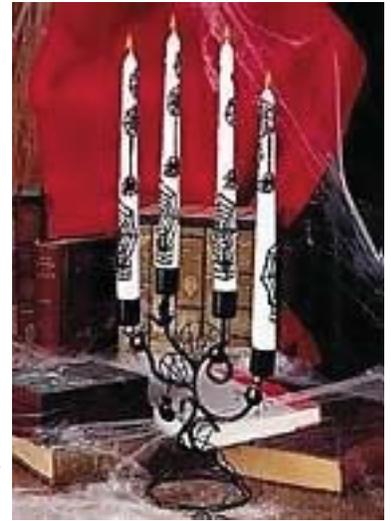
National fire safety agencies report that the bulk of candle fire incidents in the United States are due to consumer inattention to basic fire safety or to the misuse of candles. Listed below are some great tips to help prevent candle related accidents.

GENERAL SAFETY TIPS

- Extinguish all candles when leaving the room or going to sleep. Keep candles away from items that can catch fire such as clothing, books, paper, curtains, or flammable decorations. Dried flowers, cornstalks and crepe paper are highly flammable. Keep these and other decorations well away from all open flames and heat sources, including light bulbs, heaters, etc.
- Use candle holders that are sturdy, won't tip over easily, are made from a material that can't burn and are large enough to collect dripping wax. Place candle holders on a sturdy, uncluttered surface and do not use candles in places where they could be knocked over by children or pets.
- Don't place lit candles in windows, where blinds and curtains can close over them. Keep candles and all open flames away from flammable liquids.
- Keep candle wicks trimmed to one-quarter inch and extinguish taper and pillar candles when they get to within two inches of the holder or decorative material. Votives and containers should be extinguished before the last half-inch of wax starts to melt. Using a candle snuffer to extinguish candles is safer than blowing them out or using your fingers.
- Purchase only costumes, wigs and props labeled flame-resistant or flame-retardant. When creating a costume, choose material that won't easily ignite if it comes in contact with heat or flame. Avoid billowing or long trailing features.

Halloween Candle Safety Tips Continued

- Remember to keep exits clear of decorations, ensuring nothing blocks escape routes. Use flashlights as alternatives to candles or torch lights when decorating walkways and yards. They are much safer for trick-or-treaters, whose costumes may brush against the lighting.
- Use extreme caution when decorating with candles, and supervise children at all times when candles are lit. When lighting candles inside Jack-O-Lanterns, use long, fireplace-style matches and be sure to place lit pumpkins well away from all combustible items. Pumpkins can also be illuminated with small, inexpensive flashlights or glow sticks.
- Never leave the lights or any lighted decorations plugged in when you leave the house. Be sure to check the batteries in your smoke detectors. Make sure that plugs plugged into outlets and/or extension cords are plugged in safely. Always have a fire extinguisher handy during the holidays.



CHILDREN & PETS

- Never leave a child unattended in a room with a candle. A child should not sleep in a room with a lit candle. Keep candles up high out of reach of children. Don't allow children or teens to have candles in their bedrooms. Store candles, matches and lighters up high and out children's sight and reach, preferably in a locked cabinet.
- Halloween Candles Instruct children to stay away from open flames or other heat sources. Be sure children know how to stop, drop and roll in the event their clothing catches fire. (Stop immediately, drop to the ground, covering your face with your hands, and roll over and over to extinguish flames.)
- Instruct children who are attending parties at others' homes to locate the exits and plan how they would get out in an emergency. Provide children with lightweight flashlights to carry for lighting or as part of their costume.

WAX CLEANING TIPS

Wax on Carpet

This procedure may cause stains, if in doubt call in a professional carpet cleaner. Let the wax harden, then break it up and remove as much wax as possible. Place paper towels over the waxed area, then apply a hot steam iron to wick the wax into the paper towels. Protect iron with tin foil. Repeat as needed. Check iron for wax residue before using for clothing again.

Removing wax from clothing

Let harden, then remove as much wax as possible. Pour boiling water through affected area. Repeat as necessary. Do not use carpet method on clothes as it could set the candle dye in the fabric. Wax on Clothing - may cause stains, if in doubt consult a cleaning professional.

The NFPA (National Fire Protection Association), <http://www.nfpa.org/>, has great information and tips for preventing home fires.

From <http://www.halloween-online.com/safety/halloween-safety-candles.html>

Mark Your Calendar

SAACA Classic Car and Truck Show

October 4th

Location: Oro Valley Marketplace

Harvest for Hope

October 11th

Location: Oro Valley Marketplace

National Night Out

October 17th

Location: Target (First and Oracle)

Shred-A-Thon hosted by Oro Valley Community Foundation and OVPD

October 18th 10 a.m. - 2 p.m.

Location: Oro Valley Marketplace

Safe Treats

October 31st 6:00 - 7:00 p.m.

Location: Steam Pump Ranch

Fall Festival

November 8th

Location: Steam Pump Ranch

El Tour de Tucson

November 22nd

Oro Valley Tree Lighting Ceremony

December 5th

Location: Oro Valley Marketplace

Dispose-A-Med Oro Valley

December 6th 10 a.m. – 2 p.m.

Location: Target (First and Oracle)

Oro Valley Holiday Parade

December 13th

Location: Naranja between La Cholla and La Canada



www.ovpd.org

Contact Information

OVPD Crime

Prevention Unit

Northside Substation
1171 E. Rancho Vistoso

Bld., Suite 115

Oro Valley, AZ 85755

(520) 229-5080

(520) 229-5090 fax

Office Hours

Monday – Friday

8 a.m. – 5 p.m.

Sgt. Amy Graham

(520) 229-5081

agraham@orovalleyaz.gov

Ofc. Elijah Woodward

(520) 229-5085

ewoodward@orovalleyaz.gov

Ofc. Rick Rendon

(520) 229-5084

rrendon@orovalleyaz.gov

October is National Cybersecurity Awareness Month

The Internet is part of everyone's life, every day. We use the Internet at work, home, for enjoyment, and to connect with those close to us.

However, being constantly connected brings increased risk of theft, fraud, and abuse. No country, industry, community, or individual is immune to cyber risks. As a nation, we face constant cyber threats against our critical infrastructure and economy. As individuals, cybersecurity risks can threaten our finances, identity, and privacy. Since our way of life depends on critical infrastructure and the digital technology that operates it, cybersecurity is one of our country's most important national security priorities, and we each have a role to play—cybersecurity is a shared responsibility.

Like us on Facebook: www.facebook.com/OroValleyPoliceDepartment

Like the Chief on Facebook: www.facebook.com/ChiefSharp

Follow us on Twitter: www.twitter.com/OroValleyPD

**Add our Android or iPhone App, MyPD
available in the Android Market or App Store.**

