

**MARION COUNTY
SHERIFF'S
OFFICE**

Jason Myers, Sheriff
www.co.marion.or.us/so

PORCH LIGHT
CRIME PREVENTION NEWSLETTER
Spring • 2011

EMERGENCY
9•1•1

NON-EMERGENCY
503.588.5032

DRUG ACTIVITY TIP LINE
503.588.5112

GRAFFITI HOTLINE
503.566.6955

NEIGHBORHOOD WATCH
503.588.7981

VOLUNTEER COORDINATOR
503.589.3250

NEWS RELEASES
www.co.marion.or.us/so



GUNS & KIDS: BASIC TIPS FOR FIREARM SAFETY

Guns are a tool to be handled by properly trained, law abiding adults who have a reason to handle them. And whether you believe those adults should include all law abiding adults or whether you believe they should include only police and military personnel, you must make sure that children know exactly what to do when confronted with a dangerous situation.

Always lock your firearms when they are not being used. Lock ammunition in a safe place away from firearms. At an age-appropriate time, show children a gun and explain what it can do. You do not have to teach that a gun is “bad,” only that it is a tool that can be dangerous in the wrong hands. Never assume that a child will not find your gun, will not be able to fire your gun, will not know how to make it work or will remember the lessons that you have taught.

Use a good locking device. Use a gun lock device that is age-appropriate for the children living in that residence. Do not depend on a locking device as the sole safety measure. The firearm should be secured with a locking device, the ammunition stored away from the firearm and both ammunition and firearms locked in safe and secure locations.


Always assume that a firearm is loaded—and handle it that way. Even if you are absolutely certain you have emptied all the bullets from a firearm, countless people have been injured and/or killed by a bullet accidentally left in the chamber.

Continued on the next page...

OLD SCAMS RESURFACE

Lebanon Police Department warns area senior citizens of an emerging telephone scam whereby they are called by a male subject claiming to be their grandson. He reports being involved in a automobile crash in Canada, arrested and needs money for bail. Then another subject gets on the phone posing as their attorney and “confirms” the arrest. One other call received included the story of the grandson being stopped in Mexico City, found with illegal drugs in the vehicle and again needed bail money. In two of the cases, the person they were trying to scam asked questions to which the subjects had the correct answers.

This scam is preying on the emotions of seniors who want nothing more than to ensure the safety of their grandchildren. Try to remain calm despite the “emergency” nature of the call and verify the identity of the caller. Police suggest you confirm the status of the individual by calling them directly, as well as verifying the story with other family members before taking **any** action.

In all cases, they were asked to send money via Western Union. Any request to wire money through Western Union or Money Gram should be seen as a “red flag” and as an immediate tip-off that the call could be part of a scam. Funds sent via wire transfer are hard to track once received by the scammers and usually are not recoverable by law enforcement or banking officials. 

A Message from Sheriff Jason Myers

Advances in technology can bring with them unintended consequences. Consequences, in many cases, that can be prevented if the user is fully informed. Unfortunately, when modern technology crosses paths with criminal ventures, irreparable damage can occur: identities stolen, ruined credit, texting/sexting, electronic bullying, internet pictures posted that can never be redacted, solicitation of minors and cyber-stalking, just to name a few.

In a recent article by Washington County Sheriff's Office, Doreen Rivera describes another *unintended consequence*: If you have a smart phone, simply taking a picture with it and posting it to Facebook, Twitter or somewhere else on the internet, enables anyone to find the exact location of where that picture was taken. This ability is referred to as **geotagging** and is a standard feature in many phones such as iPhones, Blackberry, Android and many palm devices.

Security experts and privacy advocates have recently begun warning about the potential dangers of **geotags**, embedded in photos and videos taken with GPS-equipped smartphones and digital cameras. With **geotagging**, embedded in the image is a tag that provides the latitude and longitude of where that picture was taken. Because that location data is not visible to the casual viewer, the concern is that many people do not realize it is there and they could be compromising their privacy, if not their safety, when they post **geotagged** media on line.

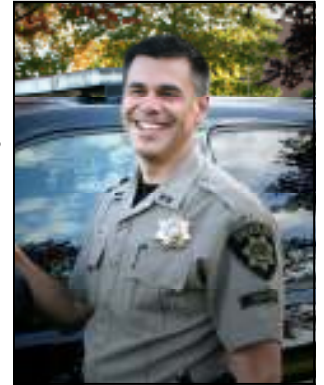
This could be a stalker's dream or a victim's nightmare. By taking a picture from your home with a smartphone and posting it on line, you are posting your exact address. Anyone viewing your pictures who knows how to obtain

the information from it, can. If you mention going on vacation or buying new items you could be creating a very unsafe situation. To see if your phone or your family phones have this feature, read the phone manual or check with the manufacturer on how you can turn this feature off. Additional information is available in a recent New York Times article at <http://nyti.ms/917hRh> or from ABC News at <http://abclocal.go.com/wabc/video?id=7621105>.

Safety first,

Jason Myers


Special Thanks to the Crime Prevention Association of Oregon and Doreen Rivera, Washington County Sheriff's Office for shining the spotlight on this potential problem.



...continued from previous page.

Never point a firearm at anyone in fun. Always point your firearm in a safe direction. Remember that a wall is not a safe direction. A distant tree in a public woods is not a safe direction. A animal that you can't identify is not a safe direction. Bullets can easily go through most walls and can injure or kill someone on the other side. It's easy to miss a tree and hit a person in the woods. Countless hunters have accidentally killed horseback riders thinking they were deer. You are liable for wherever your bullets go.

Teach children that if they see a gun they should not touch it, and they should immediately leave the area to go tell an adult. Teach children that guns are not toys, and that if a friend wants to show them a gun they should leave the area and go tell an adult. Impress upon children that this is not tattling; this could easily save their friend's life or the child's own life. Do not avoid teaching these important lessons or pretend that guns could never enter a child's life. Guns are out there and can be dangerous in the wrong hands or if handled improperly.

Do not assume other adults think the same way you do. Before letting a child play at a friend's or neighbor's house, ask if there are firearms in the home and where they are. It's a difficult question to ask, particularly of people you barely know—but asking this question could save your child's life. Remember that other adults have guns in their homes. Other adults lock guns and ammunition together. Other adults keep loaded guns in a nightstand next to their bed or even under their pillow. Other adults have not taught their own children important lessons about guns. "Other adults" will include people you believe are responsible and safe, people you wouldn't think even own guns. Many parents are reluctant to ask about guns because they're afraid to offend their friends and neighbors. Ann Marie Crowell (whose son Brian was shot to death at a friend's house) offers this advice: "I know a quick cure for embarrassment, close your eyes and imagine life without your child." 

Provided courtesy of the Crime Prevention Association of Oregon

COPY MACHINES: A SECURITY RISK?

Yes, quite possible. Most consumers do not know that the commonly used digital copier built after 2002, stores images of every document that was copied, scanned or emailed in its internal hard drive. This advanced technology has opened a dangerous hole in data security. Forensic software available free on the internet can be used to retrieve all the information on a copier's hard drive.

With the market for used copiers ever-growing as new copiers replace the old, those used copiers, sold at a substantial discount to purchasers all over the world and could pose a risk to anyone who made use of them. The digital copier industry has failed to inform the consumer of the potential of their confidential information

The digital copier industry has failed to inform the consumer ...

landing in the wrong hands through the hard drive on these copiers. Security or encryption packages are available for these copiers that would automatically erase the information on the hard drive. At an additional cost of approximately \$500, few new copier purchasers choose this feature. As users of digital copiers, the consumer needs to take responsibility for the sensitive documents they choose to copy, scan or email. But what about the potential risk for your documents to be copied by someone to whom you send them and then their copier suffering a breach of its hard drive? And Alice thought she had problems when she fell down the rabbit hole!



To view the CBS report go to:

<http://www.youtube.com/watch?v=iC38D5am7go>

IDENTITY THEFT AND ePICK-POCKETING

Without even touching your wallet, identity thieves are able to steal your credit card information. The technology exists, is readily available and can be assembled for under \$1,000. RFID (Radio-Frequency Identity) technology was introduced to make paying for items faster and easier. All major credit cards that have this technology, indicate such with the symbol shown below. It means that your card can communicate via electromagnetic waves to exchange data between a terminal and a chip installed inside of your card (or passport). Thus, by getting within a few inches of your credit card, a thief is able to obtain your credit card number, expiration date and maybe your name.

The reality is that electronic pick-pocketing is extremely time and resource intensive. Most thieves are smart enough to know that they are better served hacking into a database with hundreds of thousands of records rather than collecting them one at a time.

Identity Theft Expert, *John Sileo* believes this threat has been overblown because of equipment set-up costs, the thief has to get within 2-3 inches of your purse or wallet for 3-5 seconds, they don't get your 3-digit security code or address, and not all cards utilize the RFID/Contactless Swipe technology.



BUT it can happen, and it is worth preventing with these simple steps:

- First, check to see if you even have credit cards with the ability to beam your information to an RFID receiver, look for the circled symbol in the above photo. If not, don't worry, but continue to monitor future cards you receive.
- Next, set up account alerts and monitor your statements to cover yourself in the small chance it happens to you. If

your credit card is compromised, you can detect it immediately and take the necessary steps to contact the bank, report the fraud and cancel the card.

- If you are worried about having a credit card that can transmit your personal information, call your credit card company and request they send you a card that does not transmit or have RFID capabilities. (You know if it transmits if it has the small broadcast or sonar icon circled in the photo to the left.) Get rid of the source of the fraud!
- Never leave your purse or wallet in an easy-to-scan place. Get rid of the excess credit cards that you don't use and lower the chances that one of them will be compromised.
- For additional protection, especially for your Passport, which carries a much higher volume of very sensitive information, consider purchasing a sleeve or shield that makes RFID scanning less likely.

