

CRIME FIGHTER

The Safety Newsletter of the Oro Valley Police Department

Fourth Quarter 2015

Inside This Issue

What Should I Know About Taking Opioid Painkillers..... 4

Business Email Scam 6

Contact Information 6

Learn How to Stop Scams



Learn How to Stop Scams

In this edition of this quarter's Crime Fighter, we want to focus on frauds and cyber crime, as well as some issues that tend to come up more around the holidays. Every year, especially around the holidays, the reports of frauds and other associated crimes tend to spike. Additionally, the Department of Homeland Security has designated October as the official month of Cyber Security Awareness. They have put out a campaign known as "Stop. Think.

Connect." emphasizing the importance of being smart with how you use technology in order to avoid becoming a victim.

If your neighborhood watch group, or any organization, would be interested in contact the department about learning how to stop fraud and scams, contact Oro Valley Police Department Officer E. Woodward at 520-229-5085 to schedule a class in Fraudology 101 in Scam School!

October is Cyber Security Awareness

Below are a number of safety steps I've taken from the Department of Homeland security.

Cell Phone Safety Tips

1. Use strong passwords. Change any default passwords on your mobile device to ones that would be difficult for someone to guess. Use different passwords for different programs and devices. Do not choose options that allow your device to remember your passwords.
2. Keep software up to date. Install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent attackers from being able to take advantage of known vulnerabilities.
3. Disable remote connectivity. Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can connect to other devices. Disable these features when they are not in use.
4. Be careful what you post and when. Wait to post pictures from trips and events so



www.ovpd.org

Learn How to Stop Scams Continued

that people do not know where to find you. Posting where you are also reminds others that your house is empty.

5. Guard your mobile device. In order to prevent theft and unauthorized access, never leave your mobile device unattended in a public place and lock your device when it is not in use.

6. Know your apps. Be sure to review and understand the details of an app before downloading and installing it. Be aware that apps may request access to your location and personal information. Delete any apps that you do not use regularly to increase your security.

7. Know the available resources. Use the Federal Communications Commission website of www.ftc.gov and IdentityTheft.gov for more resources.

SIMPLE TIPS

Information Security Tips for the Workplace

1. Lock and password protect all personal and work-owned devices including smartphones, laptops, and tablets. This includes locking your computer when you step away from your desk at work. You may not always know the people walking around your office and what their intentions are. Encrypt data and use two-factor authentication where possible.

2. Regularly scan your computer for viruses and spyware and keep your software up to date.

3. Dispose of sensitive information properly and according to your organization's policies.

4. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

5. Take advantage of cybersecurity training offered by your employer or school.

6. Conceal your work badge and identification when outside of your office building, especially when out in public or when using public transportation.

Think Before You Connect.

Before you connect to any public Wi-Fi hotspot—like on an airplane or in an airport, hotel, train/bus station or café—be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. Using your mobile network connection is generally more secure than using a public Wi-Fi network.



- Guard Your Mobile Device. In order to prevent theft, unauthorized access and loss of sensitive information, never leave your mobile devices—including any USB or external storage devices—unattended in a public place. While on travel, if you plan on leaving any devices in your hotel room, be sure those items are appropriately secured.

- Keep It Locked. The United States Computer Emergency Readiness Team (US-CERT) recommends locking your device when you are not using it. Even if you only step away for



Learn How to Stop Scams Continued

a few minutes, that is enough time for someone to steal or destroy your information. Use strong PINs and passwords to prevent others from accessing your device.

- **Update Your Mobile Software.** Treat your mobile device like your home or work computer. Keep your operating system software and apps updated, which will improve your device's ability to defend against malware.
- **Only Connect to the Internet if Needed.** Disconnect your device from the Internet when you aren't using it and make sure your device isn't programmed to automatically connect to Wi-Fi. The likelihood that attackers will target you becomes much higher if your device is always connected.
- **Know Your Apps.** Be sure to thoroughly review the details and specifications of an application before you download it. Be aware that the app may request that you share your personal information and permissions. Delete any apps that you are not using to increase your security.

For small businesses:

1. Train employees in security principles. Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate Internet use guidelines, that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.
2. Protect information, computers, and networks from cyber attacks. Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.
3. Provide firewall security for your Internet connection. A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.
4. Create a mobile device action plan. Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.
5. Make backup copies of important business data and information. Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.
6. Control physical access to your computers and create user accounts for each employee. Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.
7. Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network

Learn How to Stop Scams Continued

name, known as the Service Set Identifier (SSID). Password protect access to the router.

8. Employ best practices on payment cards. Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.

9. Limit employee access to data and information, and limit authority to install software. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10. Passwords and authentication. Require employees to use unique passwords and change passwords every three months. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account



What Should I Know About Taking Opioid Painkillers

Common types of opioids:

- oxycodone (Oxycontin or Percocet)
- oxymorphone (Opana)
- hydrocodone (Vicodin or Lortab)
- methadone
- fentanyl

Ask for an alternative, such as ibuprofen or naproxone.

If your doctor recommends an opioid painkiller, understand what conditions will increase your risk:

- COPD- (chronic obstructive pulmonary disease)
- Sleep apnea
- Depression
- Anxiety
- History of addiction
- Chronic constipation

Be sure to discuss:

- Family history of addiction or alcoholism
- Working in a safety-sensitive position
- How your driving will be affected initially, and ongoing

How Do I Use Painkillers Safely?

- Treat over-the-counter and prescription drugs with caution.
- Ask your doctor, nurse or pharmacist if you have questions about a medicine
- Know the dose that's right for you

What Should I Know About Taking Opioid Painkillers

Continued

- Read and follow instructions every time
- Never take multiple medicines with the same active ingredient unless directed by a doctor
- Always put over-the-counter and prescription medicines up and away and out of sight

Talk to Your Kids about the Risks of Opioid Painkillers

- Warn them that taking a drug that wasn't prescribed to them is just as dangerous as illegal drugs
- Discuss the dangers of mixing prescription drugs with alcohol
- Explain how painkillers are made from opioids, which is similar to heroin
- Talk to their grandparents about how to safely store their medications
- Secure any painkillers, sedatives, sleep medications or stimulants in a locked drawer or container

Prescription painkiller abuse is prevalent among teens.

What are the Signs of an Overdose?

Signs of overdose include:

- Slow and loud breathing
- Sleepiness, progressing to stupor or coma
- Weak, floppy muscles
- Cold and clammy skin
- Pinpoint pupils
- Slow heart rate
- Dangerously low blood pressure
- Ultimately, death

If you suspect someone may have overdosed, call 9-1-1 immediately. He or she may appear to be sleeping, but may actually be unconscious. After calling 9-1-1, move the person into the recovery position and be prepared for CPR. If you have naloxone, administer it immediately.

How Do I Store My Painkillers Safely?

Opioid medications need to be locked up.

- Keep medicine out of sight of children and visitors
- Use a locking medicine cabinet or safe
- Return medication to your secure location after every use
- Avoid leaving medication or pill containers on countertops, tables or nightstands
- Do not keep pills in your purse, luggage, or office drawer. Locking travel cases are available to carry prescription medicines.

How Can I Get Rid of Painkillers Properly?

- Once you have finished medications, do not keep them for "later."
- Take your old pills to take-back events or collection boxes
- Ask your pharmacist about mail-back programs. Many pharmacies have drug disposal envelopes available for a small fee.
- Avoid flushing prescriptions down the toilet or drain. This can pollute water supplies and may be illegal in your state.

Never Mix Your Medications

Using alcohol and other drugs, including other types of painkillers, with opioid painkillers can intensify the effects.

- Never mix opioid medications with alcohol, sleep aids, anti-anxiety drugs or other pain relievers
- Do not take extended-release opioids as-needed for pain or more frequently than the doctor prescribed
- Talk to your prescriber and/or pharmacist to ensure you won't have drug interactions from other medications

<http://www.nsc.org/learn/NSC-Initiatives/Pages/prescription-painkillers-what-you-can-do.aspx>

Mark Your Calendar

Dispose-A-Med

Target, 10555 North Oracle Road

December 5 10 am - 2 pm

Sun City Activity Center

November 10 9 - 11 am

Safe Treats / Halloween

October 31

El Tour de Tucson

November 21 - **LOOK OUT FOR CYCLISTS**



Business Email Scam

The Oro Valley Police Department would like to make the public aware of an ongoing scam involving compromised business email accounts. In August 2015 the FBI reported this scam involved over 8,000 reported victims totaling losses around \$798 million. <https://www.ic3.gov/media/2015/150827-1.aspx>

The scam typically involves a business email account legitimately belonging to someone within your business, or a trusted partner, that sends a request to wire or transfer money. The request could also ask you to click on a link that will download dangerous software.

The Town of Oro Valley has recently seen a surge in this activity directed towards its staff. There have been no successful attempts. If you receive any financial requests from the Town that are unusual, please contact the Town at 520-229-4700, or the Police Department at 520-229-4900.

If you receive a suspicious money transfer request in the course of your business that does not relate to the Town of Oro Valley, your recommended course of action is to contact the person making the request by telephone and verify the request.

Additionally, if you have been the victim of this scam please report it to the Oro Valley Police Department. The Oro Valley Police Department will be hosting a business crime seminar in the future. Please check back for details.

Oro Valley Trivia

1. Name the German immigrant who founded a steam pump in Oro Valley?
2. What year was the Oro Valley Country Club founded?
3. When was the Hilton El Conquistador built, and whose name was on it before Hilton?

Answers:

1. George Pusch; 2. 1959; 3. 1982; Sheraton

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.

Oro Valley
POLICE

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. Marshall Morris

(520) 229-5084

mmorris@orovalleyaz.gov

