VOLUME 18 | ISSUE 2

PARTNERS IN CRIME PREVENTION

MAY/JUNE 2014

INSIDE THIS ISSUE

Ty Trenary, Sheriff
Snohomish County Sheriff's Office

3000 Rockefeller
M/S 606
Everett, WA 98201
425-388-3393
http://sheriff. snoco.org

SCAMS—SCAMMERS TAKE ADVANTAGE OF ANY SITUATION

The recent tragic landslide at Oso highlighted the danger of scammers taking advantage of the public's good will to siphon off money that victims intend to give to landslide relief. While specific scams related to Oso were not reported by the press, the incident prompted a warning by the Washington State Attorney General's Office (http://www.atg.wa.gov/pressrelease.aspx?&id=31987#.U1aiF8dOU5t).

We are often bombarded with warnings about scams. Some recent scams have included:

- An IRS scam (http://www.irs.gov/uac/Newsroom/Beware-of-Fake-IRS-Emails-and-Phone-Calls)
- A jury duty warrant scam (http://wa-snohomishcounty.civicplus.com/Archive.aspx?AMID=&Type=&ADID=3520)
- Utility scams (http://www.snopud.com/AboutUs/scams.ashx?p=1786)

Neighborhood Watches are used to preventing crimes such as burglaries and car prowls. While everyone needs to do their part by locking doors and other measures, everyone can help by keeping a lookout for potential burglars and car prowlers.

With scams, the individual may seem more isolated. We can encounter scams via email or the telephone. So we need to make a rapid decision to decline a shady offer.

Where we report scams is often not clear. Local law enforcement agencies are frequently not equipped to follow up with international fraud and scammer networks.

The barrage of warnings might be confusing. So many scammers claim to be from legitimate governmental agencies, businesses or non-profit organizations.

But the basics of what a scammer is trying to do are recognizable. The scammers want your money, either by promising something that they will not deliver or by getting access to your bank account or credit card information. It is those basics that we want to discuss in this issue.

SCAMS– PREVENTION TIPS

- *Before buying or sending money wait 24 hours to let the excitement wear off and to research the company or product.*
- *Never talk to a stranger about your personal life, especially if the stranger asks probing questions.*
- *If your heart starts beating faster, you get sweaty, and you start imagining what you would do with unexpected riches, stop! You are coming under the ether.*
- *Limited time offers or limited supply should be terms to trigger a warning about the legitimacy of the offer.*

SCAMS– HOW SCAMMERS THINK

The American Association of Retired People (AARP) has produced a handout called "The Con Artist's Playbook" (http://www.aarp.org/content/dam/aarp/money/scams_fraud/2013-10/The-Con-Artists-Playbook-AARP.pdf). It gives insight into how a con artist approaches a potential victim to convince them to give money.

Scammers, or con artists, want to put a potential victim into an emotional state that moves them to act without thinking through the logic of the situation or proposal. Scammers call this putting someone in the "ether."

They will ask questions of a prospect to find out what the prospect fears most, what they may be greedy about, and how to develop a sense of urgency in the prospect. The key is to keep the prospect in an emotional state that causes them to act without considering the logic or actual facts of a situation.

One major tactic is to appeal to a prospect's greed. The lottery scam is a good example. In this scam, you receive a phone call or email that you have won a foreign lottery. To claim your winnings you need to pay the taxes which the scammer is happy to help you do. All you have to do is send in the amount that the scammer claims that you owe and the scammer promises to send you your winnings. You send the money, the scammer forgets that you exist. The scammer sets up an expectation of easy riches that you become excited to grab before the opportunity goes away. A third party might call this "too good to be true."

Lotteries, prizes or sweepstakes that require you to pay something to claim the prize are scams.

Another element of putting prospects under the "ether" is to claim scarcity. This can come from limited time offers, scarcity of availability, or you have been exclusively selected to receive the offer.

Some scammers will use intimidation or fear to bully a prospect into paying money. Telling a grandparent that a grandson or granddaughter is in a Mexican jail and needs bail money immediately uses fear for a loved one to get them to act. Other scammers may simply harass a victim with multiple phones calls or emails to get them to pay up.

If you are being harassed, or you know of someone being harassed, call 911 and file a report with the Sheriff's Office.

SCAMS– DISASTER FRAUD

As mentioned in the first page, local, state and federal law enforcement have warned of the potential of scammers trying to take advantage of people's good will in response to the Oso landslide.

Whenever there is a disaster scammers try to take money in the guise of taking contributions for the victims.

In late April the U.S. Attorney Jenny Durkan and the Snohomish County Prosecutor Mark Roe warned of potential fraud (http://www.fbi.gov/seattle/press-releases/2014/u.s.-attorney-and-snohomish-county-prosecutor-alert-public-to-beware-of-disaster-fraud-in-aftermath-of-oso-landslide).

They made the following recommendations when considering making a contribution:

- Do not respond to any unsolicited (spam) incoming e-mails, including clicking links contained within those messages, because they may contain computer viruses.
- Be skeptical of individuals representing themselves as surviving victims or officials asking for donations via e-mail or social networking sites.
- Beware of organizations with copycat names similar to but not exactly the same as those of reputable charities.
- Rather than following a purported link to a website, verify the existence and legitimacy of non-profit organizations by utilizing various Internet-based resources.
- Be cautious of e-mails that claim to show pictures of the disaster areas in attached files, because the files may contain viruses. Only open attachments from known senders.
- To ensure that contributions are received and used for intended purposes, make donations directly to known organizations rather than relying on others to make the donation on your behalf.
- Do not be pressured into making contributions; reputable charities do not use coercive tactics.
- Be aware with whom you are dealing when providing your personal and financial information. Do not give your personal or financial information to anyone who solicits contributions. Providing such information may compromise your identity and make you vulnerable to identity theft.
- Avoid cash donations if possible. Pay by debit or credit card, or write a check directly to the charity. Do not make checks payable to individuals. Legitimate charities do not normally solicit donations via money transfer services.
- Most legitimate charities maintain websites ending in .org rather than .com

You can report fraud involving disaster relief operations through the National Disaster Fraud Hotline toll-free at (866) 720-5721 or the Disaster Fraud e-mail at disaster@leo.gov. The telephone line is staffed by a live operator 24 hours a day, seven days a week.

For more information about disaster scams go to:

http://www.aarp.org/money/scams-fraud/info-06-2013/avoiding-charity-scams-during-disasters.html?intcmp=AE-BLIL-DOTORG

SCAMS– 5 TO AVOID

1. ***Sweetheart***– *Scammer will cultivate a long distance "romance." They will come up with an emergency or business deal that they cannot finance. They ask you for money.*
2. ***Gold***– *Scammer will sell you gold. It's a sure deal. Gold always keeps its value. But he sells it so high you will not get out what you paid in.*
3. ***Grandparents***– *Someone posing as a grandson/ granddaughter asks for emergency money to get out of jail.*
4. ***Sweepstakes***– *You won a sweepstakes. Just pay the fee to claim your prize.*
5. ***Disaster***– *Help the victims of the latest disaster.*

For more information go to:

http://states.aarp.org/sc-ut-wp-money/

SCAMS– WHERE TO REPORT

Reporting scams, internet fraud, and identity theft is as important as other crimes such as burglaries, car thefts, and robberies. Internet criminals often cross government boundaries, state, federal, and international, to conduct their operations. Calling 911 to report to a deputy might help in some cases. But, you should also report your encounters to other national agencies who keep databases that law enforcement agencies can use in investigations of scammers and identity thieves.

Report suspicious scam phone calls or emails. If you are victimized by a scammer be sure to report it. The information you provide may help a law enforcement agency apprehend a crook.

Several federal agencies deal with specific aspects of financial, internet based and mail based crimes:

The Federal Trade Commission (FTC) takes complaints about identity theft, phone scams, telemarketing scams and most fraud crimes. It maintains a database that is accessed by 2,000 civil and criminal law enforcement agencies who use it in their investigations. To file a complaint go to:

https://www.ftccomplaintassistant.gov/#crnt&panel1-1

Internet crimes (cybercrimes) can include email based scams, hacking, spam, phony websites, and ransomware, **The Internet Crime Complaint Center (IC3)** takes complaints at:

http://www.ic3.gov/default.aspx

Mail delivered scams, lottery and sweepstakes, chain-letter pyramid schemes, and suspected mail theft can be reported to the **U.S. Postal Inspection Service**:

https://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx

Financial products and services including mortgages and other loans, debt collectors, banks and credit cards go to the **Consumer Financial Protection Bureau (CFPB):**

http://www.consumerfinance.gov/complaint/

Note: If your bank, debit or credit card account has been stolen or used fraudulently, immediately contact the issuer.

Investment, securities and commodities fraud can be reported to the **Securities and Exchange Commission (SEC)** at:

http://www.sec.gov/complaint.shtml

CRIME PREVENTION COORDINATORS

PRECINCT COMMANDERS

South Precinct
Lt. Rob Palmer
425-388-5262
rob.palmer@snoco.org

North Precinct
Lt. Kathi Lang
425-388-5201
kathi.lang@snoco.org

East Precinct
Lt. Monte Beaton
425-388-6262
monte.beaton@snoco.org

SHERIFF'S OFFICE CRIME PREVENTION WEB PAGE:

http://www.snohomishcountywa.gov/289/Crime-Prevention

NEWSLETTER INFO

EDITOR
Steve Moller

If you have questions regarding this newsletter or any articles that appear in it, please contact the editor at neighborhoodwatch@snoco.org

TIP LINES

Snohomish County Sheriff's Office: 425-388-3845

http://www.snoco.org/app/ssh/anonymoustips/

Crime Stoppers of Puget Sound: 1-800-222-8477