Scams and Fraud

Criminals are continually crafting new scams geared toward separating you from your savings. They do this by tricking you into handing over your cash, personal I.D., checking account numbers, and credit card information any way they can. If someone asks you for your cash, credit card numbers or other personal information—especially if you don't know them well—the safest move is to refuse their request and check with the police. The list below covers some of the most common scams we've seen in our area, but new ones are cropping up all the time:

Bank Fraud Examiner Scam – In this scam you receive a call from an alleged law enforcement professional or a bank fraud examiner with your bank. They claim to be investigating an employee and they need your help. They need you to withdraw some money and pass it to the examiner for tracking purposes. Of course, you never see the money again.

Foreign Lottery scams - No foreign country is going to go out of its way to give their money to someone overseas, but it's even less likely when you never bought a ticket in the first place!

Found Money Scams – Someone claims to have found some money – a lot of it. They want you to hold it while they find the owner. But first you must give them some hard cash to boost their faith in you. Once this happens, they switch bags, leaving you with a sack full of worthless paper.

Get Rich Scams – These involve pyramid schemes, investment scams or other get-rich quick scams. If it sounds too good to be true, that's usually because it's not true at all.

Gift card Scams – The FTC (Federal Trade Commission) reminds us that, "Gift cards are a popular and convenient way to give someone a gift. They're also a popular way for scammers to steal money from you. That's because gift cards are like cash: if you buy a gift card and someone uses it, you probably cannot get your money back. Gift cards are for gifts, not payments. Anyone who demands payment by gift card is always a scammer." For additional information on Gift Card Scams, visit the FTC website: https://www.consumer.ftc.gov/articles/paying-scammers-gift-cards

Good-Cause Scams –The offender fraudulently claims to represent a good cause—widows, orphans, police or firefighters for example--and asks for money. Or they misrepresent a cleaning product, or offer magazine subscriptions that never pan out, for sale. Often the sales are supposed to help with a worthy cause: sending kids to camp or supporting a halfway house. These may be carried out by going door-to-door, over the phone or via the internet.

Home Improvement Scams – This commonly involves someone showing up at your door who noticed your roof or driveway needs attention. They claim to be working in the neighborhood and have leftover materials so they can give you a good deal, but you must decide right now. Once they have your money they disappear, or they coat your driveway with something that does nothing to improve it.

Nigerian Scams – There are no widows, orphans, oil ministers or anyone else overseas who is legitimately going to reach out to a stranger and give them millions of dollars. This includes the Nigerian Letter or "419" Fraud, where they promise that all expenses will be reimbursed, as soon as the funds are spirited out of Nigeria.

Relatives in Emergency Situations Scams – This usually involves a variation on this: "I'm your long lost nephew, grandchild, etc., you're my last hope, I'm in big trouble, don't tell my parents, just wire some money or they'll lock me up and throw away the key." Hint: the caller is NOT your long lost relative, or anyone else you know!

Romance Scams – Although many people legitimately meet through dating services and chat rooms, there is no shortage of scam artists working this angle. They may post a false photograph, biography and age and it's nearly impossible for you to confirm or disprove its accuracy. They then spin a convincing tale of woe and you feel noble sending them money—not realizing you've been scammed. In some more elaborate schemes, they come live with you, only to fleece you in other ways once they arrive!

There are many more scams like those above and they may try to reach you through email. Here are some examples:

"Phishy" Emails - The most common form of "phishing" involves emails pretending to be from a legitimate retailer, bank, organization, or government agency. The sender asks to "confirm" your personal information for some made-up reason: your account is about to be closed, an order for something has been placed in your name, or your information has been lost because of a computer problem. Another tactic "phishers" use is to say they're from the fraud departments of well-known companies and ask to verify your information because they suspect you may be a victim of identity theft! In one case, a phisher claimed to be from a state lottery commission and requested people's banking information to deposit their "winnings" in their accounts.

Don't click on links within emails that ask for your personal information - Fraudsters use these links to lure people to phony websites that looks just like the real sites of the company, organization, or agency they're impersonating. If you follow the instructions and enter your personal information on the website, you'll deliver it directly into the hands of identity thieves. To check whether the message is really from the company or agency, call it directly or go to its website (use a search engine to find it). Do not click on email attachments you're not expecting, even if they're from people you know (or look like they're from people in your contacts – sometimes email addresses are "spoofed" to look like they're from your contacts). Lots of viruses are associated with specific types of websites, particularly those featuring pornographic material. Stay away from porn sites and you reduce your risk! Also be aware that, even if they aren't asking you for personal information, they may be planting a virus for "pharming" purposes.

Beware of "Pharming" – Is a fraudulent practice where internet users are directed to a bogus website, which mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc.

Phishy Phone Calls - Some scammers call you on the phone to try to talk you out of personal information they can use to run up charges on your credit cards. A scam some hotels have experienced, is when they receive calls to their front desk asking to be transferred to random rooms. The scammer would then pretend to be the front desk clerk, who is having trouble with your credit card, asking you to repeat the number, including the security code.

Beware of "Vishing" – Is the fraudulent practice of making phone calls or leaving messages, claiming to be from reputable companies, in order to deceive a person so they will reveal personal information, such as banking or credit card numbers.

Sign up for the national "do not call" registry. It's easy and it's free! Call (888) 382-1222, TTY (866) 290-4236 from the phone number you want to register. Unfortunately, registering by phone may not work if you live in a residential complex that uses a PBX phone system. But you can also register online at www.donotcall.gov. If you don't have a computer, use someone else's. You'll need Internet access and a working email address. The "do not call" system will send a response to that address with a link that must be clicked on within 72 hours to complete the registration.

If you are interested in something, have them send you information in writing. Do NOT give them any personal information. Check with police or other trustworthy sources.

When in doubt, always check it out! If you are in immediate danger, call 911. If the offender is at your door in the incorporated area of Eugene, call Eugene Police Non-Emergency at 541-682-5111.