



City of Eugene Police Department  
Crime Prevention  
541.682.5137  
541.682.8456 FAX

PROTECT.SERVE.CARE.

## 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—so guard that information carefully! The list below covers common scams we've seen in our area, but new ones are always cropping up.

**On-line home rentals or purchases.** Through sites such as Craigslist, Zillow, and others, scammers list houses that they don't actually own for rent or purchase at a good price. Eager tenants send money, only to later discover they've been scammed.

**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 door-to-door, over the phone or via the internet.

**Get rich schemes** – 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.

**Foreign Lottery** -- No foreign country wants to give you their money, and it's even less likely when you never bought a ticket in the first place!

**Home Improvement Schemes** – The scammers show up at your door, claiming to be working in the neighborhood. They say they have leftover materials and can give you a really good deal, but you have to decide right now. Once they have your money they disappear, or they coat your driveway with something that does nothing to improve it.

**Internet-based Romances** – 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 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 actually do come live with you, only to fleece you in other ways once they arrive!

**Found Money** – Someone claims to have found some money. They want you to hold it while they find the owner. But first you have to 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.

**Nigerian scams** – There are no widows, orphans, oil ministers or anyone else overseas who is legitimately going to reach out to a complete stranger and give them millions of dollars.



**Relatives in emergency situations overseas** – “I’m your long lost nephew, 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 cousin, or anyone else you know!

**Bank fraud examiner** – 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.

**“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.

**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. In March, 2013 a local hotel reported calls to their front desk asking to be transferred to random rooms. The scammer would then pretend to be the front desk clerk having trouble with the customer’s credit card. Could they repeat the number, including the security code?

**Shake-downs.** Callers may claim that you owe them money for products or services you never ordered, and threaten you with dire consequences unless you divulge your credit card and social security information immediately. (One version claims to come from the I.R.S. The I.R.S. will *always* send bills through the U.S. mail. They will *never* call or email demands for payment. Report fraudulent I.R.S. calls to the Treasury inspector general at 800-366-4484.

**Don’t click on links within emails that ask for your personal information.** Fraudsters use these links to lure people to phony Web sites that look legitimate. Any personal information subsequently entered goes directly to identity thieves. To check whether a message is really from a particular company or agency, call it directly or go to its Web site (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, similar to Caller ID spoofing on phones, described shortly). Lots of viruses are associated with specific types of websites, particular those featuring pornographic material. Stay away from porn sites and you reduce your risk!

**Beware of “pharming.”** With “pharming,” a virus or malicious program is secretly planted in your computer and hijacks your Web browser. When you type in the address of a legitimate Web site, you’re taken to a fake copy of the site without realizing it. Any personal information you provide at the phony site, such as your password or account number, can be stolen and fraudulently used.



City of Eugene Police Department  
Crime Prevention  
541.682.5137  
541.682.8456 FAX

PROTECT.SERVE.CARE.

**Beware of “Vishing.”** If you receive an e-mail asking you to call an 800 number related to a banking issue, don't call the number. Your credit card has a phone number on the back as do your account statements. Be safe, don't call a phone number listed in an email; instead, look up the number on your account statements.

### **Beware of Caller ID Spoofing**

Caller I.D. can be misleading. Scammers use internet-based caller ID spoofing service providers to mislead you into thinking they are legitimate callers. They pay a fee to route calls through the service, which is able to insert a different identity into the caller I.D. feature on the victim's phone. As a result it can look like the call is from the I.R.S., the F.B.I., Microsoft, your credit card company or anyone else they choose; each of these identities has been used extensively in scams over the past year. Your best protections are:

1. Hang up immediately,
2. Short of that, don't give out any financial or identity information to strangers,
3. If you've been lulled into believing the caller might be legitimate, call the alleged companies back yourself before doing any business with them – but don't use the number the caller provided. Find a number for the agency they allege to represent elsewhere, such as off the back of your credit card.
4. If the caller is selling something, or asking for a donation, and you think they are legitimate, call them first. You can invite them to mail you literature (all promises should be in writing), but you're safer if you don't give them your address – if they claim to know who you are already, they should already have that information. Do NOT give them any personal information.
5. This scam is an example of pretexting – lulling the victim into trusting the scammer by providing an impression of legitimacy, such as by showing up at their door wearing a police uniform – or hijacking the caller I.D. feature on phones. Of course all of this is illegal, but that doesn't stop the criminals. Spoofing can be reported to the Federal Communications Commission (FCC) on-line or at 1-888-225-5322 or the Federal Trade Commission at [www.ftc.gov](http://www.ftc.gov)

**Join the national “do not call” registry.** Call (888) 382-1222, TTY (866) 290-4326 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](http://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.

**When in doubt, always check it out!** If the offender is at your door, call Eugene Police Dispatch at 541-682-5111. For more crime prevention information, call EPD at 541-682-5137.

