Skyline Rural Watch Newsline

Mailbox: newsline@srnpdx.org
Urgent: alert@srnpdx.org
Phone: (503) 621-3501

June 19, 2018

Good Advice on Spotting Scammers

It happens all the time. Someone gets hacked and everone in their contact list get's a scam email. Many of our neighbors recently received a scam email, appearing to be from one of our neighbors, that was requesting a loan due to a theft while they were traveling.

A scam I heard of that a friend almost fell into, was on renting a house. They called the number on the sign in front of the rental. The sign had been placed there by the scammers. My friend called the number, the sammers weren't able to show the house at that time, but offered to hold the house for them if a down payment was sent. The market was tight, it was a good deal in the neighborhood they were looking in, they almost fell for it.

- Some new scams include:
  - Voter/polling scams. An email or phone call claims you must "confirm" your address and social security number to check your voter registration.
  - Fake job posts on Craigslist. They steal your private information and compromise your identity, rather than have actual jobs to fill.
  - Fake Facebook promotions. They claim to promote a company by handing out free gift cards in exchange for your email address. They sell your information to spam companies and never send any promised gifts.
  - Fake websites. They often falsify their "Like" count to make them appear popular and legitimate.
  - Fake news sites. Some scam artists in foreign countries use commonly available blogging software, stock images, and cheap hosting to create news/blog sites. They use outrage-based tactics by feeding preconceived notions with phony evidence (such as Photoshopped photos) to entice email, passwords, and ad-clicks from users and friends they share the fake news with. Crime groups can take advantage of the sites which operate outside of US legal jurisdiction, and can use them as a platform for collecting personal information.
  - Fake Facebook profiles. Accepting a Friend request could expose your location, photos, and friends to communicating with the fake profile.

Examples:

- Scammers will contact you, claiming to know you:

    - If someone contacts you by any means (phone, email, postal mail, text messages), never automatically assume they are who they say they are.
    - If someone claims to know you, but they do not even know your name, do not respond.
    - Usually, scammers use a scare tactic, such as issuing a fake "warning" that your bank account or domain name has been compromised. They offer a link to click, sending you to their site where they can ask for your bank or password information. Remember, no legitimate website (Facebook, banks, credit agencies, travel companies, etc.) will ever request you confirm your identity or password by email. Even if the email looks real, they may not be. If you do receive a scary notice from your bank, credit card, government, or service provider, simply call them on your own to verify the legitimacy of the notice. Never click links within emails claiming to be from a bank or credit institution, even if they appear are legitimate.
- Scammers who "solicit victims":
    - If you see a "sponsored" post on your social media account, do not assume it is a legitimate operation within the US. Anyone can post "sponsored" ads on social networking sites.
    - If you see a job ad without trusting the source (such as someone on Craigslist), do not assume they actually have a job to offer. Never give any personal information before scheduling an interview. Prospective employers will NEVER request your social security number and driver's license BEFORE an interview.
    - "You just won a sweepstakes," or "you must be one of the first 1,000 Facebook or Twitter fans to win a gift card to a popular retailer." Unless you heard about it from the actual retailer's website or their actual Facebook/Twitter fan page, they are fake and you will get nothing except tons of spam and identity thieves will put a big target on you.
    - If a new Twitter page or Facebook page claims to be a company or person, but asks you to enter any personal information, forward something to friends, or "sign up" to get something, do not do it unless you know for certain they are legitimate.
    - If you receive an official-looking letter in the mail notifying you that your car's warranty or domain name is about to expire, never respond to those. Data miners can find personal information from vehicle registrations, homeowners' financing firms, and domain name registries.
    - If you use a popular online dating website and get a message or read a profile from an attractive person who prefers you contact them through another dating/social website, they could be a scam. Scam artists specialize in hooking people in, then changing the communication method to hide their tracks from authorities.
- Scammers who Email:
    - If an unfamiliar person uses a free email account like @yahoo.com or @gmail.com, never assume they are who they say they are.

    - If someone you do not know personally uses an email account at a domain name you never heard of, look up their contact information:
        1. Use Domaintools.com to look up their email address, and scroll to the bottom and view their registration information.
        2. If their mailing address looks suspicious, foreign, or contains the words "proxy" or "privacy", they could be a scammer.
        3. If you are still unsure, run a google search for the domain or email address and see what shows.
    - Sometimes scammers will send fake invitations to events, or fake emails showing your order is on hold and must be claimed. Again, confirm the information by contacting the company yourself via their website and/or phone, and never click on links within the emails.
    - Scammers may claim they know you, but you don't know them. Those emails often include an offer.
    - Scammers may offer illegal services or products by email, such as Viagra without a prescription.
    - More often than not, fraudulent/fake emails will have typos, grammatical and spelling errors, formatting issues, websites with errors, and may claim to know you indirectly using words like "friend," "sir" or "madam".
    - If an email appears confusing or illegible, just ignore it. If a website doesn't function as you expect, be suspicious of it.
- Chain Email Hoaxes and Facebook Fan Pages:
    - Anytime you get an email suggesting you will benefit by forwarding it to a certain number of friends, those are friendly hoaxes designed to waste people's time and clog up people's inboxes. If a Facebook Fan Page claims you will get money or fame by referring 10 friends to fan the page, that is a scam and you will receive nothing. If you received such an email or Facebook Fan alert from one of your friends, let them know they fell victim of an Internet hoax.
- Scammers who approach you in-person:
    - Legitimate people collecting money for a cause will have fliers, contact numbers, and websites because they want to get their word to as many people they can. Scammers will likely have dirty or mutilated signs, or no signs at all. They often use a "hard luck" story or use their children as props for their scams.
    - All legitimate people love to show their credentials. They are proud of their work, position, and accomplishments. So if you see an unfamiliar face, simply ask for their credentials, licenses, or identification before giving them any money or information. Scammers often come prepared with excuses why they have no documents, because they are hiding something.
    - Ask for their office phone number, take out your cell phone and call them right away. Someone trying to steal something from you will likely not give out any of their personal information, such as their real phone number. If their cell phone does not ring when you call it, they probably gave you a

fake number.

Never send money orders, checks, cash, phone numbers, and your social security number to anyone you met on the Internet. Use PayPal, Square Cash, or dozens of other money transfer services which give legal protection from fraud.

Use a credit card when possible. Debit cards (also known as check cards) are harder to contest after the money leaves your account.

If you decide to meet someone in-person, such as buying/selling goods on Craigslist or if you met someone through an online social website, be sure to meet in a public place or an area where there are other people around.

Always ask questions.

FROM SKYLINE RIDGE NEIGHBORS WEBSITE - SRNPDX.ORG

SKYLINE VOICES:

http://www.srnpdx.org/: Local author's essays, opinions, ponderings and musings. We welcome anyone in the neighborhood to submit a blog post. Submit to: web_edit@srnpdx.org

CLASSIFIED AD and SRN FORUM:

srnpdx.org - Find It: http://srn.freeforums.net/http://srn.freeforums.net/

EVENTS:

srnpdx.org - Calendar: http://www.srnpdx.org/calendar1.html

Resource Directory:

As a service to neighbors, SRN publishes a listing of local government agencies and businesses in the Skyline Resource Directory. Follow the links in this section to view its contents and learn how to add a business or agency listing.

Listing of organizations and businesses herein does not imply any endorsement of SRN nor does it imply a lack of endorsement for similar organizations or businesses not included.
COMMUNITY LINKS:

Skyline Grange: http://www.srnpdx.org/skyline-grange-894-0
Forest Park Conservancy: http://www.forestparkconservancy.org/
Linnton Community Center: http://www.linnton.com/lcc.asp
Linnton Neighborhood Association: http://linntonna.org/
West Multnomah County Soil and Water Conservation District: http://wmswcd.org/
Skyline School: http://www.pps.k12.or.us/schools/skyline/
Lincoln High School: http://www.pps.k12.or.us/schools/lincoln/

About the Newsline: Skyline Rural Watch Newsline is a part of Skyline Ridge Neighbors (SRN) and has been produced since June 1994 as a means to communicate neighborhood information. The Newsline is produced by Laurel Erhardt (editor) with help from Miles Merwin, Libby Merwin, and Sen Speroff
The Newsline depends on you as a source of accurate information about local crimes, upcoming events, and other news pertinent to the area. If you have information you would like considered for the Newsline, you may do so by e-mailing the information to newsline@srnpdx.org, or leaving a message at (503) 621-3501. Urgent, timely items (crimes, lost pets) should be emailed to alert@srnpdx.org.
If you would like more detailed information about any item on the Newsline, request that information & SRN will e-mail it to you if available.
You can subscribe to the Newsline at the Skyline Ridge Neighbors Website, SRNPDX.org. Tell your neighbors about this

free Newsline service.
About Skyline Ridge Neighbors: SRN is a neighborhood association serving much of unincorporated northwest Multnomah County and some adjacent areas within the city of Portland. SRN is registered as a neighborhood association within Multnomah County, registered as a non-profit public benefit corporation with the State of Oregon and approved as a 501(c)(3) non-profit organization under the IRS Code. SRN is operated by volunteers and with donated funds entirely.
If you would like to donate to SRN in support of its activities, such as this free Newsline service and the publication of its quarterly Skyline Ridge Runner, send your donation to “Skyline Ridge Neighbors”, c/o John Eskew, 15604 NW Rock Creek Rd, Portland OR 97231 or donate with credit card thru PayPal - http://www.srnpdx.org/ Contributions are tax deductible to the extent allowed by law.