



NEIGHBORHOOD WATCH

BEWARE – THESE SCAMS DO EXIST!



| SCAMMERS APPROACH | WHAT YOU SHOULD KNOW |
|---|---|
| The scammer presents himself as a law enforcement or IRS officer to create fear and a sense of urgency. To avoid arrest you are instructed to pay a fine for not showing up for jury duty, or pay IRS back taxes, or pay bail money for unpaid ticket. | Government agencies do not call, send unsolicited emails, text messages, or use social media to discuss personal information. Only recently has the IRS begun calling individuals on the phone. However, before any agency calls you they will send you a letter. If you haven't received a letter, HANG UP! It's Shrewd, not rude. |
| You receive an email from the scammer indicating you have won a Sweepstake or Lottery and you need to send money for the taxes, or a friend on vacation has lost a passport or had a wallet stolen and is asking for money. They want money via gift cards or MoneyGrams. | DO NOT EVER SEND MONEYGRAMS OR GIFT CARDS TO STRANGERS! Call your friend to verify their situation. The IRS has plans in place for people that owe back taxes. Notification of sweepstakes and lottery winnings are always delivered via US mail. |
| With the "Hi Grandma Scam", scammer creates fear and urgency by impersonating a grandchild that needs money for legal fees, to get out of jail, or is in the hospital due to an accident, or is stranded in a foreign country. | Ask for identifying information only the grandchild would know. You and your grandchild can create a "safety" word in advance that only the two of you would know. Also, you can call the parents. If you can't verify you are actually in contact with your grandchild, HANG UP AND REPORT THE INCIDENT TO THE LINCOLN POLICE AT 916 645-4040. |
| Microsoft/Apple Scam – your personal computer screen freezes and a message saying your firewall is breached or your computer is infected with a virus. You are directed to call phone number to enlist the help of a Microsoft/Apple technician to correct. The scammer then accesses and infects your computer with malware and corrupts your files and convinces you to pay for repairs and/or insurance. This is an opportunity to also steal your identity. | DO NOT CALL THE OFFERED NUMBER! Immediately turn off your computer and unplug it from your network. Reboot your computer. If a restore screen directing you to call a number for service appears DO NOT FOLLOW ITS DIRECTIONS. Call a trusted computer service company to restore your computer. You can also obtain a referral from Neighbors InDeed. |
| You receive an email from Banks, AT&T, Yahoo, Apple or other business entity that appears to be legitimate. The scammer wants to verify your personal information because your account has been "compromised, locked, or involves a security problem" and may want you to turn over control of your computer to him. | NEVER CLICK ON A LINK IN AN UNSOLICITED EMAIL! Businesses will notify you by US mail. Your first line of defense is the Delete key. Watch for incorrect grammar or punctuation. Email addresses in the US end in @xxx.com or @xxx.net, but @xxx.edu for Universities/Colleges is very popular with scammers. Foreign email addresses end in letters that identify the country i.e., @xxx.my (my = Malaysia). |
| Aggressive door-to-door solicitor claims to have a relationship with PG&E, water company, alarm company, or pest control company. He wants personal information for an immediate purchase or he wants to update the alarm system or check your house for pests. | DO NOT ALLOW STRANGERS INTO YOUR HOME! Talk through the door or window. Solicitors are required to carry a Lincoln Business License. Ask to see it. Otherwise, CLOSE THE DOOR! Contact Lincoln Police at 916 645-4040 or if threatened, call 9-1-1. |

Contact Alerts Team at SCLHAlerts@watch.lincal.org or

View recent alerts on www.SCLHWatch.org

Revised July 8, 2018