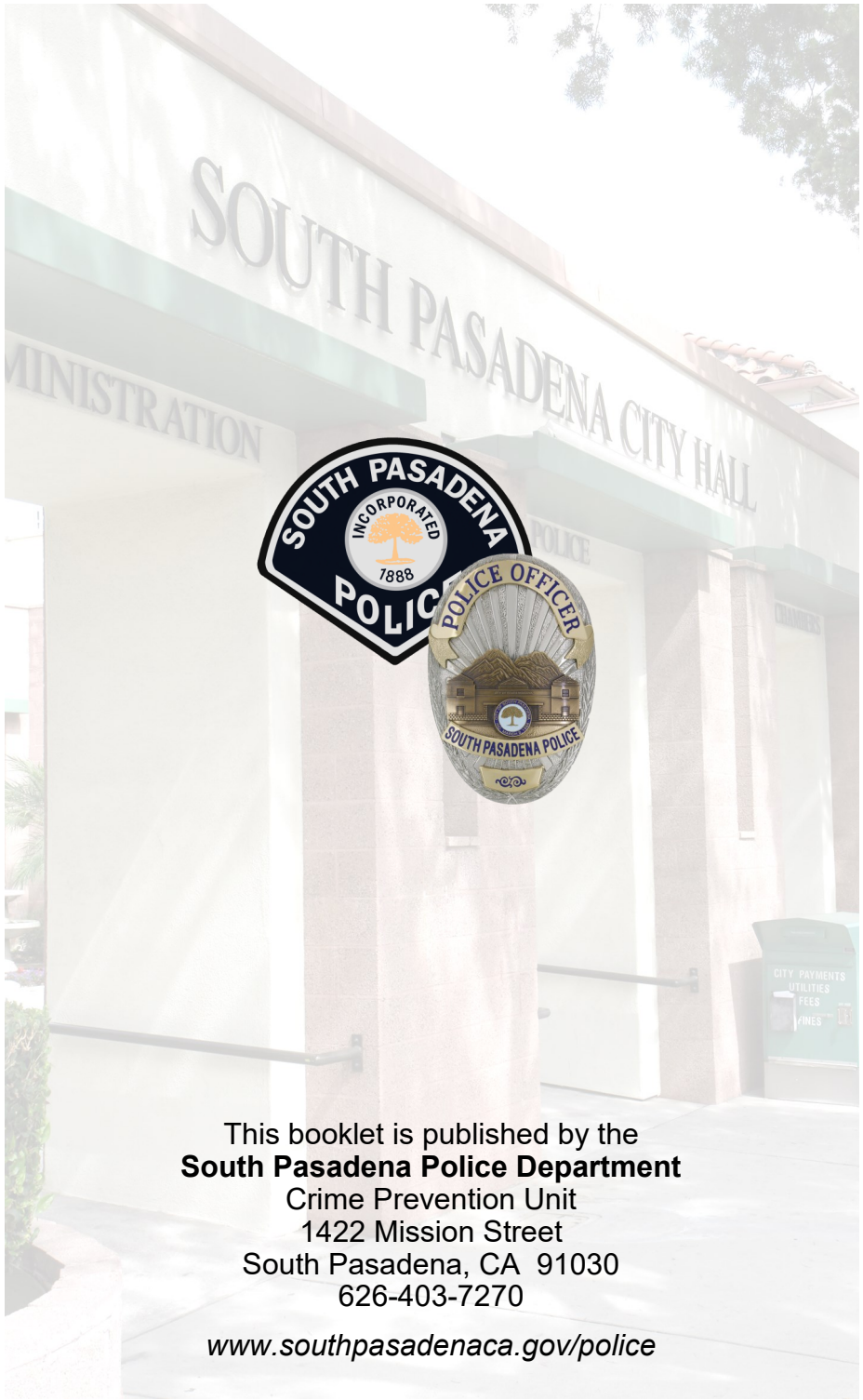


This booklet is published by the
South Pasadena Police Department
Crime Prevention Unit
1422 Mission Street
South Pasadena, CA 91030
626-403-7270

www.southpasadenaca.gov/police

Phishing - Home Repairs - Distraction
Theft - Foreign Lottery - Fake Accidents
Nigerian "419" Letter - Instant Wealth
Emergency Relative in Distress
Telemarketing Scams - Sweepstakes
Fake Check - Instant Winner! - Pigeon Drop -
Phishing - Home Repairs - Distraction

SCAMS & CONS

A Residents Guide to Prevention

Phishing - Home Repairs - Distraction
Theft - Foreign Lottery - Fake Accidents
Nigerian "419" Letter - Instant Wealth
Emergency Relative in Distress
Telemarketing Scams - Sweepstakes
Fake Check - Instant Winner! - Pigeon Drop -
Phishing - Home Repairs - Distraction
Theft - Foreign Lottery - Fake Accidents
Nigerian "419" Letter - Instant Wealth
Emergency Relative in Distress
Telemarketing Scams - Sweepstakes
Fake Check - Instant Winner! - Pigeon Drop

Courtesy of the
South Pasadena Police Department

Brian Solinsky
Chief of Police

Scams and Cons
A Residents Guide to Prevention

Table of Contents

Introduction 1
Defining Scams and Cons 2
History 2
Myths 3
Types of Scams and Cons
- Home Repair 4
- Fake Accidents 5
- Distraction Thefts
  - Residential Burglary 6
  - While Shopping 6
- Foreign Lottery 8
- Advance Fee (Nigerian Letter) 9
- Sweepstakes 10
- Fake Charities 11
- Pigeon Drop 12
- Relative in Distress 14
- Fake Check 16
- Phishing 18
- Pre-Paid Debit Card (IRS) 20

What to do if you are a victim 21
Conclusion 22
General Safety Tips 23
Resources for victims 24

This booklet was designed and published by the
South Pasadena Police Department, Crime Prevention Unit

Revised 2019

INTRODUCTION

Most people think they are too smart to fall for a scam or a con. However, according to the Federal Trade Commission in 2011, scam and con artists were able to swindle over 25 million US adults.

Scam and con artists don't discriminate, regardless of race or age. They look for the old and young, male and female. Seniors are often targeted because they are usually lonely and compassionate. Scam and con artists use this to their advantage by trying to befriend them. They offer promises of quick wealth to seniors who are on a fixed income and are out to steal their savings. People in their 20s are more often victims to scams than seniors, but lose less money than seniors.

Unlike other types of crimes, scams and cons are non-violent crimes and involve the suspect being friendly. Because scam and con artists work by deception, they have excellent communication skills to try to gain one's confidence.

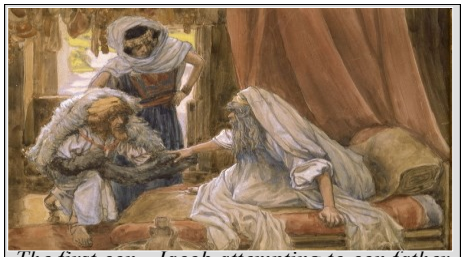
This booklet was developed to help residents know the various types of scams and cons that are being used today. South Pasadena is not immune as we have had many residents fall for each of the scams and cons listed in this booklet. Variations of these scams and cons are used each year so the best prevention is to recognize the various types of scams and cons so you won't be a victim.

Did you know?
According to the FBI, Health Care/Health Insurance Fraud, Prescription Drugs and Funeral Scams are the top scams for seniors.

DEFINITION

"Con Artist" is short for "Confidence Artist", meaning the suspect defrauds the victim by gaining their confidence. "Scam" is short for "swindle", meaning theft by a trick or trade. Both are used synonymously as they imply the same thing.

HISTORY



The first con. Jacob attempting to con father in to believing he was his brother.

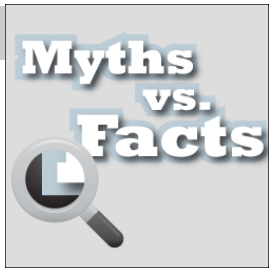
Scams and Cons are not new and have been around for a long time. In fact, the first scam/con is often said to have occurred back in biblical times. In the Book of Genesis, Jacob attempted to con his father in to believing he was his brother Esau.

Throughout time, scam and con artists have searched for unsuspecting victims by walking around stores and homes. The use of mail, faxes and telephones allowed scam and con artists to work from home to deceive victims. Now with the internet, scam and con artists can access victims from anywhere in the world. No longer do con and scam artist have to spend money on stamps or phone charges. Email is free, and con and scam artists can even access the internet at free internet locations.

Did you know?

One of the most famous cons to occur was the sale of the Brooklyn Bridge? Back in the 1900s, George Parker conned immigrants into purchasing the Brooklyn Bridge. George Parker performed this con several times before he was arrested.

MYTHS



The first step in spotting a scam or con is to clarify some myths about them. How would you answer the following myths?

All companies, businesses and organizations are legitimate? True or False?

False! Many scam and con artists will use similar sounding names to mislead their victims.

All internet websites are legitimate? True or False?

False! Anyone can make a website. Scam and con artists will often create a website that resembles a real company to mislead their victims.

There are shortcuts to wealth that only a few people know? True or False?

False! Other than winning the lottery, there is no shortcut. Scam and con artists will say anything to lead you to believe that you can make a fortune by a small investment.

Scams and cons always involve a large amount of money? True or False?

False! Some scam and con artists will look to get a small amount of money from their victim, but scam/con a large number of victims. In fact, not all scams and cons involve cash. Some are after personal information so they can later steal your identity.

It is easy to spot a scam or a con? True or False?

False! Scam and con artists have excellent communication skills which allow them to gain your confidence easily. They may also flash large amounts of money to help further gain the victims confidence.

TYPES OF SCAMS AND CONS

HOME REPAIR

The scam/con artist will knock on your door and claim they are working in the area and have extra supplies (usually driveway or roof repair). They will give you a free estimate and claim it will be the cheapest price you can find. They also claim they are a licensed contractor and provide you a license number. They then ask for a large deposit of up to 50% up front.

REALITY: They overcharge for the work they perform and should they actually do the work on the spot, the work will be of low quality. Or, if you pay the large deposit, they will give an excuse to leave (usually to purchase more supplies) and won't return. The contact number they provide you will be either a bad number or they will give excuses why they haven't returned. The contractor license number will also be fake or belong to another company.

TIPS:

- ***Always get a written contract that has the contractors name, contact information and contractors license number on it.***
- ***Any work over $500.00 requires a contractor's license.***
- ***Down payment for work cannot exceed $1,000.00 or 10% (whichever is less) of the contract price.***
- ***Verify a contractor's state license through the "Contractors State License Board" website (www.cslb.ca.gov).***
- ***Don't fall for high pressure sales. Always get three bids to compare the prices.***
- ***If they claim to be in the area working, ask for the address so you can see their work.***
- ***Ask for referrals and check on all of them.***
- ***Be suspicious if they claim to work in California but have out of state license plates on their vehicle.***
- ***In addition to a state contractor's license, a contractor must also have a South Pasadena City Business License to conduct business in the city.***
- ***A building permit may also be required depending on the work needed. You can call the South Pasadena Building and Planning at 626-403-7220 to check if the work you need requires a building permit.***

FAKE ACCIDENT

The scam or con artist will be walking around parking lots looking for a motorist that is backing out of a parking stall. They will approach the rear of the car and hit the car, claiming you hit them. They then ask for money for medical bills instead of calling the police. They tell the victim about how their car insurance will increase and the police will get involved to scare them into just paying them cash on the spot. There may be a second person involved who claims they were just walking by and witnessed the whole thing.

REALITY: If the person really was hit by a vehicle, they would want the fire department to come out for medical assistance. You would also want the police department to respond to take a report for the injury. Documentation is the best prevention you can have document all the involved parties. Scam and con artists don't want to provide their information to the police department. Don't worry about insurance premiums, knowing that the police and fire department responded to investigate the accident should give you peace of mind.

TIPS

- ***Don't give money out to anyone who claims to be injured.***
- ***Always be sure to look while backing up, and make eye contact with pedestrians.***
- ***If you are involved in an accident that involves an injury, the police must take a report.***
- ***Aftermarket back-up cameras can be purchased and installed on your vehicle.***

Always look before reversing

Aftermarket back-up cameras are available

DISTRACTION THEFTS

Distraction thefts can occur at home or while you are in a business, typically grocery shopping at a market. Usually, there are at least two suspects, one to distract you while the other takes your valuables.

DISTRACTION THEFTS AT HOME

The distraction thefts at home occurs when the first person knocks on your door and claims to be a utility worker, city inspector, or a contractor working at a neighbor's house. This first person may ask to enter your home to check on utilities and keep you in one room of the house while his partner comes in and goes to your bedroom and takes valuables. They may also claim to show you something in your rear yard and keep you there as his partner goes inside your house to take valuables.

DISTRACTION THEFTS AT MARKETS

The distraction thefts at the markets are similar. First, they look for females who place their purse in a shopping cart. The first person will distract the female by either engaging them in a conversation or ask for their assistance in retrieving an item off the shelf. While the female victim is looking away, the second person swipes the wallet out of the victim's purse and walks away. The female victim often doesn't know her wallet has been stolen until she goes to pay for groceries. By that time, the thieves have already made charges to the victim's credit card.

REALITY: Although the distraction theft at home can be classified as a burglary it shows how a variation in the scam/con can lead a thief into your home. As all scam and con artists, they will engage in a friendly conversation with you long enough for you to lose focus on your purse.

DISTRACTION THEFT PREVENTION TIPS

TIPS WHILE AT HOME:

- ***Don't let anyone that you don't know into your home or allow them to enter the side or rear yard of your residence.***
- ***If you didn't call for utility or city service, ask to see their work ID. Don't trust a uniform by itself.***
- ***If they claim to be a contractor working at a neighbor's house, contact your neighbor to verify. You can also call the employer's work to verify service. Don't trust the number they provide.***
- ***Remember a city worker will never ask to go inside your home. City services ends at the meters! Water, gas and electrical lines from the meter to your house is YOUR responsibility.***
- ***If a water or gas main really is broken in the streets, contact the Public Works Department at 626-403-7240, the Gas Company at 800-427-2200, or Southern California Edison at 800-655-4555 to confirm it.***
- ***City workers will usually have a colored shirt with the city logo on it. All city workers will have a city identification card.***
- ***If you suspect any suspicious activity, call the police department at 626-403-7297.***

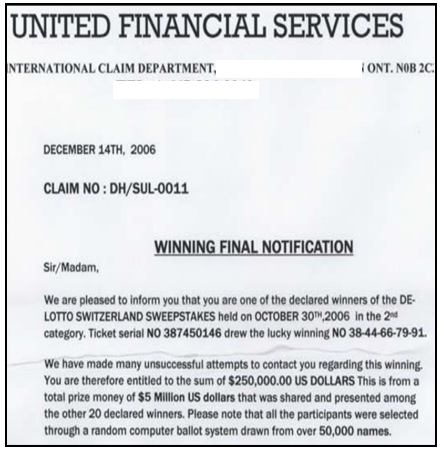
TIPS WHILE OUT SHOPPING

- ***Don't leave purses unattended.***
- ***Keep your purse closed up.***
- ***Consider bringing just your wallet with you and keep it in your pocket.***
- ***Keep your purse strapped around you rather than leaving it in a shopping cart.***
- ***Don't let any distraction keep you from focusing on your purse.***

While out shopping, strap your purse around you for better security

FOREIGN LOTTERY

This was a common type of scam that was mailed and faxed to victims, although with the internet it is often emailed as part of a Phishing scam.



UNITED FINANCIAL SERVICES

NTERNATIONAL CLAIM DEPARTMENT, ONT. N0B 2C.

DECEMBER 14TH, 2006

CLAIM NO : DH/SUL-0011

WINNING FINAL NOTIFICATION

Sir/Madam,

We are pleased to inform you that you are one of the declared winners of the DE-LOTTO SWITZERLAND SWEEPSTAKES held on OCTOBER 30TH,2006 in the 2nd category. Ticket serial NO 387450146 drew the lucky winning NO 38-44-66-79-91.

We have made many unsuccessful attempts to contact you regarding this winning. You are therefore entitled to the sum of $250,000.00 US DOLLARS This is from a total prize money of $5 Million US dollars that was shared and presented among the other 20 declared winners. Please note that all the participants were selected through a random computer ballot system drawn from over 50,000 names.

The scammer sends a letter claiming you won a lottery in a foreign country (usually Canada) and all you need to do to claim it is to first pay for service fees, taxes and associated costs. If you send the "advance fees" the scam/con artists will continue to ask for additional fees and soon your bank account will be drained. You will never see the "lottery winnings".

Should the scam/con artists call you on the phone, they may have another person come on the phone and claim to be an attorney and help verify the scam. This second scam/con artist will be very convincing and sound authoritative.

REALITY: How can you win a lottery you never entered, especially in a foreign country that you probably didn't go to? Scammers and con artists send thousands of these letters out hoping to get at least one response. It only takes one victim to comply to make them happy.

TIPS:

- ***It is illegal to play out of country lotteries by mail or phone.***
- ***Shred or delete the email/letter and any unsolicited junk mail.***
- ***Should you receive a phone call saying you "won" a foreign lottery or any lottery you did not play, hang-up.***
- ***Use an answering machine to help screen your calls. Most scam/con artists won't leave messages.***
- ***Once you respond, the scammer will forward your name and contact information to other scammers to send you more lottery winnings.***

ADVANCE FEE ("NIGERIAN LETTER")

The "Nigerian Letter" scam, also know as the "419" (after the section of the Nigerian penal code that addresses fraud) as well as the "Advance Fee Fraud" is one of the oldest scams around.

Originally, this type of scam dates back to the 1800s in Spain where the scam/con artist would ask a victim for money to help bribe prison guards to get a family member out of prison. The scam/con artist would promise huge rewards. Fast forward to the 1980s when many US residents were getting mailed letters from Nigeria requesting assistance in transferring huge sums of money out of the country. While the letters looked official, the scam/con artist would promise a large percentage of the money if they assist and they always encourage you to keep this "confidential". All that the victim needed to do was to provide your bank account and help pay various fees. Once the victim paid the fee, the scam/con artist would always ask for additional fees to help transfer the money. Of course, you never see the money.

Today, the "Nigerian Letter" scam is often emailed to victims, although we occasionally see them mailed.

REALITY: Do you know the person who sent the letter to you? How could they possibly know to pick you out of all the persons living in the world? Would anyone be willing to send a large amount of money to someone they don't know, or haven't met in person? The scam/con artist sends thousands of these letters/emails out hoping to find at least one victim to comply.

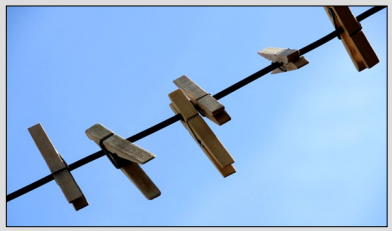
TIPS

- ***Should you receive any unsolicited mail, shred it! Or, if emailed delete it.***
- ***Never respond to any unsolicited mail or email. If you reply back on email, you just provided the scam/con artist with a verified email address and you will start to receive more scams and cons.***
- ***The Secret Service investigates this type of scam. Remember, the South Pasadena Police Department has no jurisdiction out of the country.***

SWEEPSTAKES WINNER

"Congratulations! You are the winner!" These simple words are enough to have victims fall prey to this type of scam. Similar to the Foreign Lottery, this type of scam/con is mailed, faxed, or emailed to victims worldwide. It states that you are a winner of a valuable prize and you simply have to pay for processing fees, shipping, taxes, etc. The prize is usually worth far less than all the associated fees you paid to get the prize.

REALITY: Like the lottery scam, how can you win if you never entered a sweepstakes? However, the sweepstakes scam operates in a "grey" area of the law. You do receive a product, but the product is valued far less than the fees you paid. For example, you respond to a sweepstakes letter saying you won a new solar heater and pay $50.00 in fees to get the prize. The thrill of winning a valuable new solar heater turns to disappointment when you open the package and see a string and a set of clothes pin.



Congratulations!
You won a new solar heater

TIPS:

- ***Shred or delete the email/letter and any unsolicited junk mail.***
- ***Should you wish to enter any sweepstakes be sure to read all terms and conditions associated with the sweepstakes. Be on the lookout for any hidden costs. Your information may also be shared with other companies so you may get more calls and sweepstake notifications.***
- ***Research the company that is conducting the sweepstakes. Remember just because they may have a website doesn't mean they are legitimate.***

FAKE CHARITIES

As long as there are real charities seeking donations, there will always be fake charities also seeking donations. Fake charities donations go straight into the scam/con artists pockets! Fake charities will have similar names to actual charities. The names are so close that most victims won't notice the difference. They often come out during holidays, after a disaster or memorials for fallen heroes to take advantage of your generosity. Many times the scam/con artist will say they are assisting the local police or fire department, implying the South Pasadena Police or Fire Department.

REALITY: Fake charities divert needed money that would have gone to an actual cause to assist a needy family. Police and fire departments **CANNOT** solicit donations! The South Pasadena Police Officers Association (SPPOA), which represents the employees of the police department, mails out a letter to solicit for donations. The SPPOA does **NOT** solicit by telephone or email.

TIPS:

- ***Should anyone call you claiming to be from the SPPOA, or local police and is seeking a donation, hang-up!***
- ***Verify the charity name to confirm it is legitimate.***
- ***Don't let the emotions of an event dictate your donation.***
- ***Consider going to the organization directly to make the donation.***
- ***Donate to recognized charities that you know.***

Would you donate to these organizations?

These are all fake organizations!

PIGEON DROP

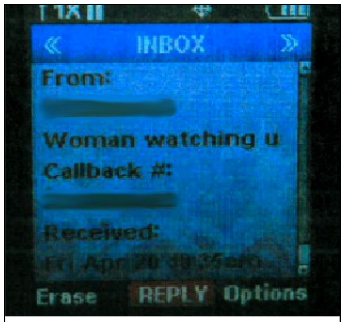
The "Pigeon Drop" is so called because the victim is "Pigeon" and involves at least two suspects. In this type of scam, the suspects contact the victims in person, usually at a public place like a store or in a parking lot.

The first suspect will contact the victim and say he urgently needs their help because they are leaving the country today. The suspect has a large sum of money, or a piece of gold (or other valuable metal) to donate to a church, or they have a winning lottery ticket that they cannot cash because they are in the country illegally.

They ask the victim to help them find a church to donate the money to and, in return, the suspect will give some of the money to the victim. The suspect will show the victim a bag of money to help convince the victim the story is true (the outside of the bundle of money will usually be a $100.00 bill and the rest will be $1.00 bills). The second suspect would suddenly appear and help convince the victim that the first suspect story is true.

Actual bag of money shown to a victim of a Pigeon Drop Scam

The first suspect will ask both to provide "good faith" money before he would share the money. The second suspect will play along and provide some money. Both suspects will then pressure the victim into going to the bank and withdrawing money.



Actual text message between two suspects in a pigeon drop scam, warning of a witness watching them

Once the money is provided by the victim, the first suspect would than place all the money in a bag and make a switch and give the victim a similar looking bag full of newspaper.

The suspects have the victim hold the bag as the suspect makes an excuse to leave, as they either need to use a restroom or need to buy medicine.

Once both suspects leave, the victim would be left with the switched bag of newspaper.

The piece of gold or valuable metal would turn out to be a piece of lead painted gold or silver. The winning lottery ticket turns out to be counterfeit or has the incorrect date on it.

A fake gold bar

REALITY: Would a complete stranger really trust a person they don't know with a large amount of cash? Any person that asks you to give them money and then gives you money back should raise a red flag.

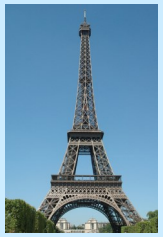
A classic example of a "Pigeon Drop" scam is shown in the opening scenes in the 1973 movie "The Sting" with Robert Redford and Paul Newman.

TIPS:

- ***If the person really needs help, direct them to the police department for assistance.***
- ***Your safety is important, don't let any stranger into your car.***
- ***Don't believe any story that a stranger tells you, especially if it involves a large amount of cash.***
- ***Be cautious of the unexpected second con artist who just happens to walk by and verifies the first person's story.***
- ***Never provide a large sum of money to a stranger.***
- ***If anyone asks you to provide "good faith" money up front, walk away and call the police.***

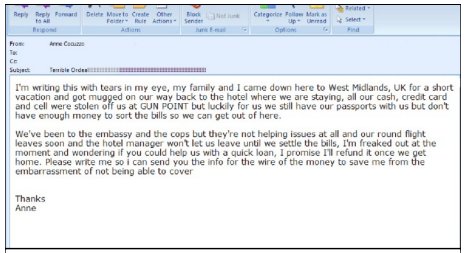
Did you know?

One of the most famous landmarks in the world was sold by a con artist? In the mid-1920s, a con artist named Victor Lustig conned a victim into buying the Eiffel Tower for scrap metal.



RELATIVE IN DISTRESS

This type of scam/con has increased over the years, most likely thanks to the internet.



Distress email sent to a victim

In this scam/con the suspect will contact the victim, either by phone or email, and impersonate a relative of the victim, usually a grandchild. The suspect may just say "Grandma, it is me, I need your help." The victim will assume it is their grandchild and say the name of their grandchild to the suspect. The suspect will then just agree.

They claim they are out of the country and in trouble (they have been arrested, involved in an accident, etc.) and need you to immediately send money to them to help pay for hospital bills, legal fees, or bail money.

At times, another scam/con artist will get on the phone and pose as an attorney, doctor or police official verifying the story and needs you to send money right away by either a pre-paid debit card or wire transfer.

The suspect urges the victim to keep this confidential and not tell anyone. The suspect may provide the real name of a grandchild to help make the story believable. After the victim sends the money, the suspect will contact the victim again and ask for additional money for other fees. The more the victim sends, the more the suspect will ask for additional money.

The victim will later discover their grandchild never left the country.

This type of scam is made more believable if sent by email because they may have your correct email address and may have the correct email address of a relative.

REALITY: Scam and con artists are counting on your emotions to help assist them. No police official will ever ask you to send them money, especially by wire transfer, cash or pre-paid debit card.

RELATIVE IN DISTRESS TIPS

- ***Resist the urgent need to provide assistance without verifying the story. Ask relatives if their grandchild really is out of the country.***
- ***Never initiate your grandchild's name. Let them provide the name to you.***
- ***If the caller is claiming to be a doctor or police officer, ask for their name, business name and a call back number. Don't call them back until you can verify their story.***
- ***Verify the identity by asking questions that only your grandchild will know, and don't provide any personal information.***
- ***Don't believe the person's story even if they have the correct email address of a relative. Email addresses can be easily "spoofed", or modified to show one email address when in fact it is going to another email address.***
- ***Be cautious about sending money overseas. Remember the police department has no jurisdiction out of the country.***
- ***Statements or emails that say "Don't tell mom or dad", or "Urgent, send money ASAP" should raise concerns.***
- ***Be cautious of what you, your family and friends post about you on social networking website. You may not have any social networking websites, but your family, relatives and friends sure do. More than enough information can be found to learn about you from what your family and friends post. Email addresses and names can be easily found through social networking websites. With a little online research, more information can be found about you.***

Be cautious of what you, your family and friends post about you on social networking websites

FAKE CHECK

This is one of the most common scam/cons we see today. There are several variations of this type of scams.

In one variation, the suspect will respond to an internet ad that the victim is selling a product. The suspect sends a check over the amount of the asking price. When the victim discovers the discrepancy the suspect apologies for the error and asks to send the excess amount back, or to another person. After the victim sends the excess amount to the suspect, the victim later discovers that the check is counterfeit.

In another variation of the scam, the victim replies to an online employment ad and the suspect sends the victim a check and asks the victim to deposit the check into their own bank account and immediately send money to other people, mainly out of state. Again after complying with the suspect's instructions, the victim learns that the suspect's original check is counterfeit.

REALITY: Would any consumer really send a check over your asking price in error? Why would they ask you to forward the difference to another person? Online employment is growing, but be cautious if they are too eager for you to start work by forwarding money to out of state people.

EARN MONEY WITHOUT LEAVING YOUR HOME!

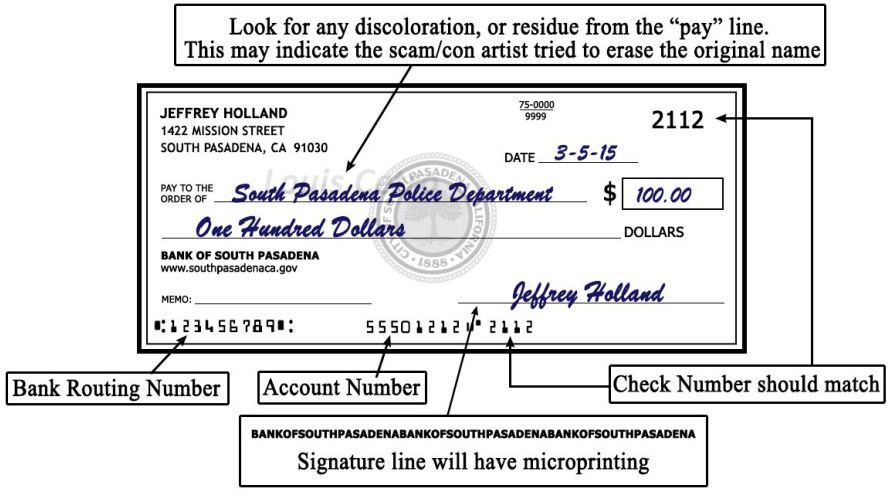
MAKE $1000 A WEEK!
NO EXPERIENCE NEEDED

CALL 800-555-1212 NOW!

Credit card thieves will often solicit "work at home schemes" by saying you can make money by forwarding merchandise to other people across the country. Soon you start receiving items, usually electronics, and are told to mail them to various people. What you don't know is that the merchandise you are receiving is bought by stolen credit cards and shipped to you. When the police investigate the stolen credit card, your address is revealed as the shipping address and they come knocking on your door.

FAKE CHECK SCAM TIPS:

- ***Remember that you are the seller, you dictate the terms of sell not the buyer.***
- ***Don't accept checks for more than your selling price. Return the check and ask for a correct one.***
- ***Cashier's check can also be counterfeit. A scam/con artist can purchase a legitimate one, then duplicate it several times.***
- ***Detecting counterfeit checks can be difficult. Always make sure checks clear your bank before sending any merchandise.***
- ***Banks may not be able to immediately identify a counterfeit check. The check must be returned back to the source bank to verify that the check is genuine.***
- ***Make sure the address on checks matches the return address on the envelope.***
- ***If you receive a check from an employer you just replied to online, again make sure the check clears your bank before you forward any money, or make any purchases.***
- ***Be cautious of any work at home schemes. Be sure you read all contracts and understand the job.***
- ***While it is difficult to detect a counterfeit check, here are some quick tips to look for to make sure a check is genuine:***

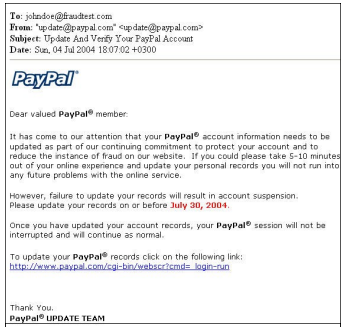


- Be cautious of spelling errors
- Be cautious if the check smells of chemicals. Chemicals can be used to erase ink.
- Look for perforations along the edge of the check

PHISHING

"Phishing" is an internet type of scam/con where the scam/con artist develops a website that resembles a legitimate company's website. These "lookalike" websites are used to lure victims into providing their personal information. Scam and con artists will send an email that resembles an official company and pose as your bank, a business, internet provider, Fed Ex or UPS delivery, etc. The email contains a hyperlink they want you to click and be directed to their "lookalike" website. The victim enters their personal information and with one click, the scam/con artist has everything they need to steal your identity, or siphon money from your account.

REALITY: Banks and related companies will not send you an email asking you to enter your personal information. Hyperlink names that are shown on emails can be easily changed to read any name. However, the actual link is revealed if you hover your cursor over the hyperlink (remember don't click the link!). The actual location of where you will be directed to will be shown at the bottom of your web browser. Also, clicking on hyperlinks may invite malware and spyware on your computer, which may allow unauthorized access to your computer.



To: johndoe@fraudtest.com
From: "update@paypal.com" <update@paypal.com>
Subject: Update And Verify Your PayPal Account
Date: Sun, 04 Jul 2004 18:07:02 +0300

PayPal

Dear valued PayPal® member:

It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before July 30, 2004.

Once you have updated your account records, your PayPal® session will not be interrupted and will continue as normal.

To update your PayPal® records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

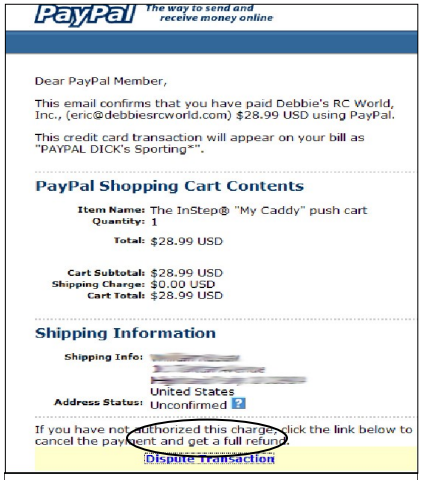
Thank You.
PayPal® UPDATE TEAM

Example of a Phishing email

Malware (refers to Malicious Software) is software that gathers information or disrupts computer operations. Spyware is where the thief is gathering information from your computer without your knowledge. Both are considered viruses and very damaging. Malware such as "Keystroke Loggers" can track your keyboard letters that you type, thus gaining passwords. "Worms" can embed itself into the deep roots of your computer and can affect the operation of your computer. "Trojan Horses" hide viruses within a program so you won't even see it. "Ransomware" is an annoying pop-up that fills your entire computer screen and demands that you send money in order to remove it. Each time you reboot the computer, the pop-up appears.

PHISHING TIPS:

- ***Remember links can be disguised. Read the company name carefully, it is easy to overlook a similar name, i.e., "Paypall" instead of "Paypal".***
- ***If you suspect your account has been comprised, call them directly with the number you have on file. Never trust the contact information on the email.***
- ***If you get an email or pop-up message that asks for personal or financial information, do not reply or click the link in the message. Just delete it! If you reply to a Phishing email, all you have done is to confirm a valid email address to the scam/ con artist.***
- ***Don't email personal or financial information. Email is NOT a secured means of transmittal. Remember, email is nothing more than an internet "postcard".***
- ***Make sure your anti-virus software is up to date and routinely scan your computer.***
- ***Be cautious of "FREE" programs as they may contain hidden viruses (called "Trojan Horse").***
- ***Microsoft Windows has a free built-in malware removal software called "MRT" (Malicious Software Removal Tool). Just type "MRT" in the command line from the start menu to run it. This does NOT replace you anti-virus software, it is another type of software to protect your computer from malware.***



PayPal The way to send and receive money online

Dear PayPal Member,

This email confirms that you have paid Debbie's RC World, Inc., (eric@debbiesrcworld.com) $28.99 USD using PayPal.

This credit card transaction will appear on your bill as "PAYPAL DICK's Sporting*".

PayPal Shopping Cart Contents

Item Name: The InStep® "My Caddy" push cart
Quantity: 1
Total: $28.99 USD

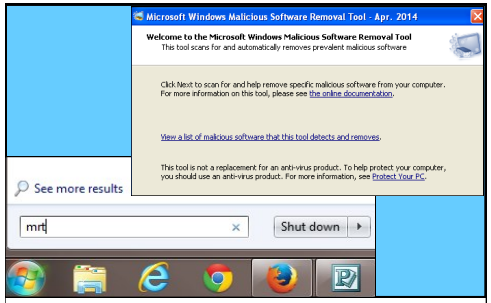
Cart Subtotal: $28.99 USD
Shipping Charge: $0.00 USD
Cart Total: $28.99 USD

Shipping Information

Shipping Info:
United States
Address Status: Unconfirmed

If you have not authorized this charge, click the link below to cancel the payment and get a full refund.
Dispute Transaction

Be cautious of hyperlinks in phishing emails. Hovering your mouse over the hyperlink will reveal the true destination



Type "MRT" from the start menu to run Malicious Software Removal Tool

PREPAID DEBIT CARDS

We have seen an increasing number of this type of scam/con occurring. There are different variations but the scam/con artists wants you to purchase a pre-paid debit card (Mostly "Green Dots") and provide them with the card number and code.

The most common type of this scam/con occurs when the scam/con artist calls you at home and says they are an Internal Revenue Service (IRS) Agent and provides you a fake badge number. They claim that you owe for back taxes and they demand that you immediately pay a fine, or you will be arrested. The scam/con artist is usually very aggressive on the phone and sometimes provides the last four digits of your social security number to make their story more believable. They ask that you go to a store and purchase a "Green Dot" debit card, then call them back with the card number.

We have also seen the scam/con artist pose as an Edison employee and threaten to turn off the power to your house or business because your electric bill is past due. Again, the scam/con artist will demand that you pay immediately or your power will be turned off.

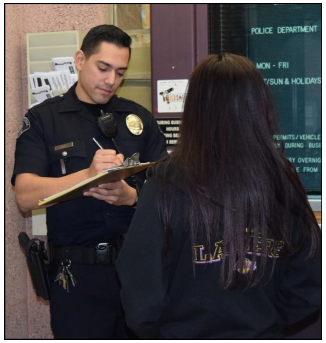
REALITY: The IRS, Edison, or any other utility worker will never demand payment by a pre-paid debit card. Utilities will always mail overdue notices as well as the IRS who will mail letters should you owe for back taxes. If the IRS had a warrant for your arrest, they would not call, they would come to your door. Local police departments will not come to arrest you on a federal warrant.

TIPS:

- ***Should you be concerned if you have an overdue utility bill call the utility company directly. Never call a number the scam/on artist provides you. Instead, call the number that is on your utility bill.***
- ***If you think you owe for back taxes and have not received a letter, you can call the IRS (www.irs.gov) at 800-829-1040.***
- ***Should the scam/con artist provide you with the last four digits of your Social Security Number, you may be a victim of identity theft. You should immediately obtain your credit report to verify your credit history.***
- ***The Treasury Inspector General for Tax Administration (TIGTA) is a branch of the US Treasury Department and handles fake IRS scams.***

WHAT TO DO IF YOU ARE A VICTIM?

Report the Scam/Con



Many victims feel embarrassed that they fell victim to a scam/con and do not report the crime. However, if you are a victim immediately report it. Helping to report the crime will assist others to be aware of a scam/con occurring locally. This will help reduce the chances that another victim may fall prey to the scam/con artist.

If you were a victim where the scam/con artist contacted you in person ("Pigeon Drop", "Distraction Theft"), immediately report it to the police. If the police are immediately contacted, there is a chance that officers may catch the scam/con artists in the area.

While we do offer online police reports, this type of crime should be reported in person to an officer. Please do not use our online reporting for crimes of scams and cons.

In addition to reporting the crime to the police department, you should also file a compliant with the appropriate agency (Federal Trade Commission, Contractor's State License Board, Treasury Inspector General for Tax Administration, etc.).

Internet scams can be reported to the FBI's Internet Crime Complaint Center (www.ic3.gov). The IC3 unit is part of the FBI and is staffed by both FBI agents and intelligence specialists. Reports are investigated and reviewed to compile intelligence information for both law enforcement and for public awareness.

Take Action

If you fell for a "Phishing" scam, or clicked on a link on an email or pop-up, you may have a virus on your computer. **Don't** conduct any online banking or payments. Immediately update your anti-virus software and run a full and complete scan of your computer. If you continue to get pop-ups, or have "ransomware" you may have to seek technical assistance.

If you feel your personal information has been compromised, obtain a "freeze" on your credit by contacting the three major credit bureaus (Experian, Transunion and Equifax). Also, obtain and review your credit report to determine any unauthorized accounts. You are allowed one credit report per year for free at www.annualcreditreport.com

If your credit cards or checking account was used or stolen, contact the bank to cancel the credit card or check. If you wired money, immediately contact your bank to stop the transaction.

Because pre-paid debit cards are paid in advance, they are like cash. Unfortunately, there is little recourse once you provide the card and code number to the scam/con artist. Therefore, it is important to be cautious before making any payment with a pre-paid debit card.

Warn Others

Help spread the word about the various types of scam/cons that exist. Remember that there will always be some variations to each scam/con.

CONCLUSION

Many residents continue to think they are too smart to fall for a scam or con. But, sadly, many South Pasadena residents continue to fall victim to these various types of scams and cons each year.

With the internet, many scam and con artists continue to locate victims all over the world. Scam and Con artists particularly want you to send money overseas where US law enforcement has little to no jurisdiction. Even if they were arrested, extradition from some countries can be difficult. Some scam and con artists provide partial truth, so they work in a "gray" area of the law and prosecution can be difficult.

The best protection against con and scams is to know the various types that are being used today. Variations will always occur so it is important to be able to spot a scam and con immediately. The quicker you can identify a scam or con, the less likely you will become a victim.

GENERAL SAFETY TIPS TO REMEMBER

Here are some other general safety tips to remember:

- ***If an offer seems too good to be true, assume that it is too good to be true.***
- ***Don't be pressured into buying or investing in anything. Ask a trusted friend or family member before investing your hard earned cash.***
- ***Never provide account information over the internet or telephone, unless you originated the call.***
- ***Use secured websites when making purchases over the internet. Look for either a padlock symbol at the bottom of your web browser, or "https:" in the URL.***
- ***Run antivirus software on your computer at least weekly.***
- ***Don't keep financial or other important documents in the hard drive of your computer. Computer viruses like malware and spyware can gain access to personal information, or "crash" your computer where you may not be able to recover your data. Store all important files on an external hard drive.***
- ***Shred any papers that have your personal information. This also includes any pre-approved bank card offers you receive in the mail. A thief can simply sign your name, designate a change of address on the application and mail it back to the bank.***
- ***Don't open your door to strangers. You can talk to them through the door.***
- ***A stranger can claim to be anyone, always ask for identification to prove who they work for.***
- ***Don't use public computers, or places that have free internet ("Wifi") to conduct banking or shop online. These are not secured connections and vulnerable to cyber attacks.***
- ***Change passwords regularly and use a combination of letters, numbers and special characters. Avoid using simple words, or dates of birth. Never use a social security number as a password.***

HELPFUL RESOURCES

The following is a list of helpful resources for residents:

Annual Credit Report
www.annualcreditreport.com
For a free copy of your credit report (allowed once a year).

Contractors State License Board
www.cslb.ca.gov
Check the status, or verify a contractor's license number.

California Department of Consumer Affairs
www.dca.ca.gov
Provides consumers with assistance in filing complaints against licensed practitioners and business. You can also check the status of a business license.

Credit Bureaus
The three recognized credit bureaus can place a fraud alert on your credit.
Equifax, www.equifax.com, 800-766-0008
Experian, www.experian.com, 888-397-3742
Transunion, www.transunion.com, 800-680-7289

Federal Bureau of Investigations Internet Crime Complaint Center
www.ic3.gov
Reporting of internet scams to the FBI. Reports are processed for investigative and intelligence purposes for law enforcement and public awareness.

Federal Trade Commission
www.ftc.gov
US Government consumer protection agency. File a complaint and also provides safety information.

Internal Revenue Service
www.irs.gov. 800-829-1040
If you think you owe, or have questions on back taxes.

National Crime Prevention Council
www.ncpc.org
A great resource for any topic on crime prevention.

Scambusters
www.scambusters.org
A resource to know about current scams and prevention tips.

Southern California Edison
www.sce.com, 800-655-4555
Verify if you are late on payments, or to verify an unscheduled service person at your door.

Southern California Gas Company
www.socalgas.com, 800-310-2355.
Verify if you are late on payments, or to verify an unscheduled service person at your door.

South Pasadena Finance
www.southpasadenaca.gov, 626-403-7250
(Mon-Thur, 7:30 AM to 6 PM)
To verify a city Business License

South Pasadena Planning and Building
www.southpasadenaca.gov, 626-403-7220
(Mon-Thur, 7:30 AM to 6 PM)
To verify if you need a city Building Permit

Treasury Inspector General for Tax Administration
www.treasury.gov/tigta, 800-366-4484
Reporting IRS impersonation scam. Also provides safety information.

SOUTH PASADENA POLICE DEPARTMENT
1422 Mission Street, South Pasadena, CA 91030
EMERGENCY 9-1-1
NON-EMERGENCY 626-403-7297