Frauds, Scams & Senior Safety

Stay Alert, Long Beach—
If you see something, say something!



presented by

LONG BEACH POLICE DEPT.
SENIOR POLICE PARTNERS

Presentation Goals

By the end of this presentation, you will:

- **Be Aware** of common forms of fraud and scams
- Stay Alert and know how to spot them
- **Be prepared** in how to handle them
- **Pass it on** to friends, family, loved ones, and work places





By the Numbers



Fraud affects every generation differently.

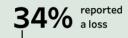
CONSUMER SENTINEL NETWORK DATA BOOK 2020 SNAPSHOT

MILLION **REPORTS**

TOP THREE CATEGORIES

- 1 Identity Theft
- 2 Imposter Scams
- 3 Online Shopping and Negative Reviews

2.3 million fraud reports



\$3.4 billion total fraud losses

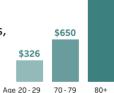
\$306 median loss

Younger people reported losing money to fraud more often tha..



Age 70-79

But when people aged 70+ had a loss, the median loss was much higher.



\$1,300

Identity Theft Reports

Imposter Scams



1 in 5 PEOPLE

\$1,228 million reported lost

\$850 median loss

Government **Benefits**

2916%

Applied For\ Received

4%

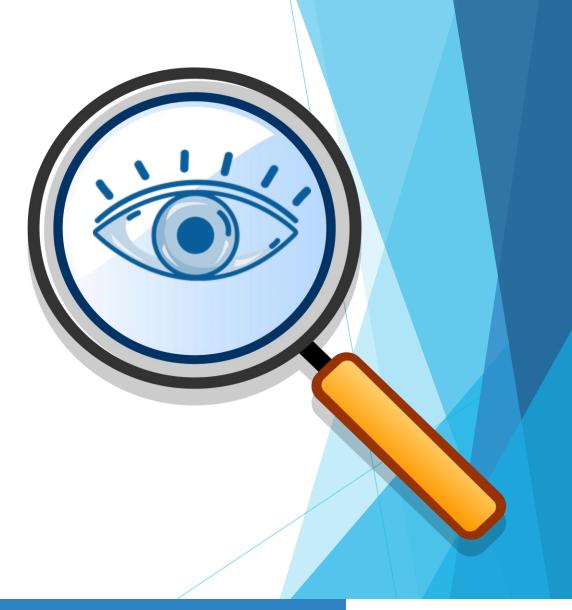
Evading the Law

FEDERAL TRADE COMMISSION · ftc.gov/

Latest stats found @ ftc.gov/explored



How would we spot "identity theft"?

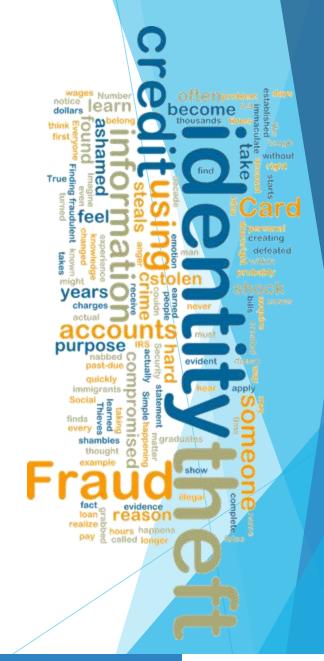






Identity Theft Defined

- Identity theft are all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.
- Most common ways this happens, as stated by the DOJ:
 - **Shoulder surfing** watching/listening-in from a nearby location as you punch in or state your credit card number over the phone.
 - Pre-approved credit cards in the mail that have been discarded without tearing up the enclosed materials.
 - **Unsolicited email or "spam"** that promises some benefit but requests identifying data in return.







Protect Yourself from Identity Theft

Spotting Identity Theft

- Monitor and report anything suspicious to the financial institution:
 - Read your statements
 - Read your explanations of benefits
 - Watch your bills
- Check your credit reports for free, annually!

How do you protect your information?

- Tear up or shred documents before throwing them away
- Don't leave mail in the mailbox for too long
- Mail letters from the post office or an official mailbox, not the mailbox on your porch
- Give your Social Security number only when you MUST (and ask why you must)
- Use strong passwords online (combination of letters, numbers, symbols)





Be Prepared! Use Free FTC Recourses

 Track the latest scam alerts at <u>ftc.gov/stay-</u> connected Obtain free annual reports online at <u>annualcreditreport.com</u>

• Or call 877-322-8228

 Register to opt-out of receiving telemarketing calls at <u>donotcall.gov</u> Get free informational publications to post or distribute (e.g., in the lobby of a senior center or apartment complex) at <u>bulkorder.ftc.gov</u>

CONSUMER ALERTS



FREE CREDIT REPORTS



DO NOT CALL REGISTRY



FREE PUBLICATIONS







Different Types of Scams & Fraudster Tactics

SCAMP

- Fake Check Scams
- Healthcare Scams
- Charity Fraud
- Caregiver Fraud
- Tech Support Scams
- Home Repair Scams
- Mass Mail Scams
- Job Search Scams

- Imposter Scams
- Grandparent Scams
- Lottery or "You've Won" Scams
- Online Dating or Sweetheart Scams
- Social Security Phone Scams
- Mortgage & Foreclosure Scams
- Money Mule Scams
- ...and more!





What do all scam artists do?



Deceive and prey on emotional wants, needs, fears and vulnerabilities



Use different forms of anonymity **often** without any face-to-face interaction



Want you to act fast and not think too much about it or tell anyone else

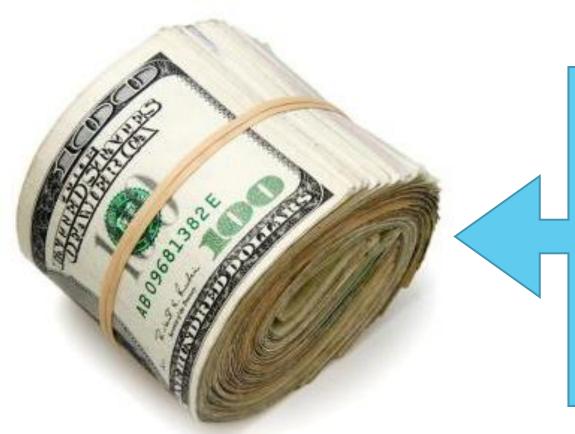


Use forms of payment that aren't traceable or retractable





Would you hand over a roll of cash to anyone?



- Wired Money,
- Checks,
- Gift Cards,
- Pre-paid cards,
- Cryptocurrency,

are all equivalent to handing over cash!
Once it's gone, it's gone.





Fake Check Scams

- When you deposit a check, banks have to make the deposited funds available to you within days. It's the law.
- But uncovering a fake can take weeks. When found, it's returned back to the customer as a counterfeit.
- By then the Scammer has your money, and any overdrawn funds will need to be repaid to the bank.







Protect Yourself from Fake Check Scams

WHAT TO DO:

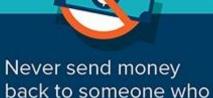
Be wary.

Talk to someone you trust and contact your bank before you act.



Never take a check for more than your selling price.





sent you a check.



Spot this scam? Tell the Federal Trade Commission: ftc.gov/complaint



Source: Federal Trade Commission | FTC.gov



When I say, "Imposter Scams," what do you think of?







Different Types of Imposter Scams

They say...

- "Grandma, I need money for bail. Don't tell mom."
- "I'm calling from [Official-Sounding Company]! You've won a fabulous prize! But first, there's a fee..."
- "I wish I could come meet you, but I don't have enough money for a plane ticket."
- "I'm calling from [Official-Sounding Charity] regarding disaster relief for [recent humanitarian crisis]. Will you consider making a cash payment today?"

How would you respond?

- Hang up
- Ask mom
- Tell them "I have a personal rule to not send money to people"
- Tell the charity "I have a personal rule to not give money over the phone. If you send me something in writing, I'll consider it"





Sweetheart Scams

- Another variation of the Imposter scam
- Never wire money, put money on a prepaid card, or send cash to an online love interest. You won't get it back.
- Pass this information on to help your friends and family recognize this scam before it happens to them.

Signs of an online dating scam



Professes love quickly.

Claims to be from the U.S., but is overseas for business or military service.



Asks for money, and lures you off the dating site.



Claims to need money

— for emergencies,
hospital bills, or travel.

Plans to visit, but can't because of an emergency.





Keep Alert!

- Don't respond to unsolicited phone calls
- Scrutinize any claims made over social media or email
- Don't trust what's on the Caller ID
- Look up customer reviews before any first-time purchases on a website
- If it sounds too good to be true, it usually is
- If it sounds overly dramatic and involves money, it usually is only about the money
- When in doubt, talk to a trusted person







Looking for Opportunity

Scammers love to "help" when there is a natural disaster, shortage, or health scare that makes national news.



Natural disasters (hurricanes, tornadoes, wildfires, floods, earthquakes)



Emerging or significant outbreaks of diseases (COVID-19, Pandemic Influenza)



Human-caused disasters (bioterrorist attacks, nuclear/radiation accidents)





Government or Healthcare Scams

They say...

- "You need a new Medicare card to continue coverage."
- "There's a problem with your social security number or account..."
- "I'm from the IRS and you owe back taxes."

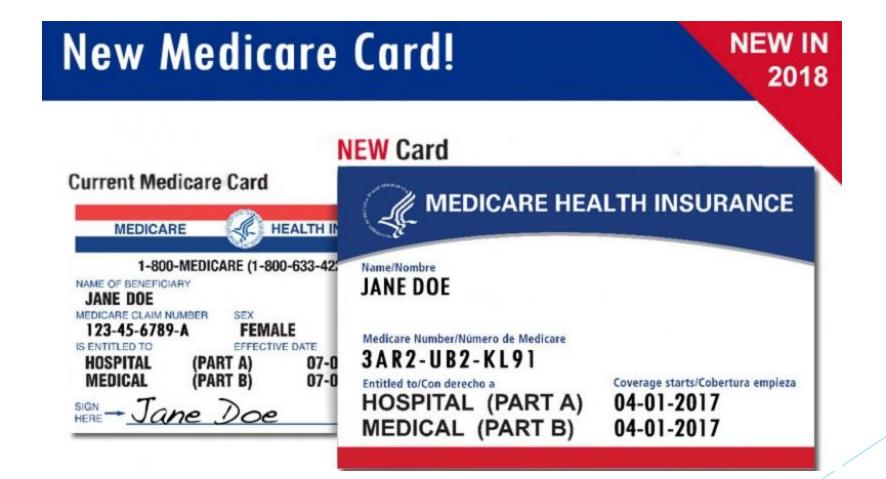
Want to be sure?

- Call Medicare at 800-MEDICARE or visit medicare.gov
- See the latest from the Social Security Administration (SSA) at <u>oig.ssa.gov</u>
- Call our Long Beach-based IRS branch at 562-491-7751
- Or talk to someone you *trust*!





Mass Mailing Scams







Government Workers Would Never

- Threaten you
- Suspend your social security number or Medicare card
- Demand immediate payment from you
- Demand personal information
- Ask for payment in cash, gift cards, or wire transfer
- Notify you over the phone, *especially* on first contact

...but scammers will





Common COVID-19 Scams

What is Happening

- Fake and unauthorized at-home testing kits being sold/distributed.
- Scammers posing as a government authorities (like FEMA) to charge or collect payment for vaccine, funeral services, or other healthcare access needs.
- Fraudulent websites are being built to promote fake treatments, bogus in-demand products, or scam stimulus and charity themed websites.

How to be sure...

- Check the FDA's lists of authorized tests for home use before you buy!
 - Antigen diagnostic tests
 - Molecular diagnostic tests
- Check reputable/known sources to confirm any claims made.
 - www.usa.gov/coronavirus
 - www.coronavirus.gov
- See the latest info on health scams and fraud alerts:
 - oig.hhs.gov/fraud





Beware of Fake Testing Sites!

Fake Testing Sites

- Fake testing sites look real, with legitimate looking signs, tents, hazmat suits.
- Sites will offer "free tests"—but then bill you later and sometimes never give the test that was promised.
- The sites are also taking people's personal information for identity theft purposes (including SSN's, credit card and other healthcare information).

What you can do

- ► **Get a referral.** Only go to the locations referred by your doctor or our local Health Department:
 - www.longbeach.gov/covid19
 - COVID-19 Info Line: 562-570-4636
- Check the source. Hear about a new testing site through a neighborhood social media group? That neighbor could be a scammer.
- Not sure if a testing site is legit? Call our non-emergency dispatch line to report it at 562-435-6711.





Fraud in the Technology Age

- Phishing is where a scammer impersonates a business or a person to trick you into giving out your personal information, such as passwords, credit card numbers, or bank account information.
- > **Spoofing** is when a caller disguises the information shown on your caller ID to "spoof" the name and/or number to appear as though they are calling as a certain person from a specific location.
- Malware is the general term for any program that is designed to damage, disrupt, or hack a device. Computer viruses and ransomware are malware and are one of the ways that scammers can get access to your personal information.







What would you look for when trying to spot an email scam?







How to Determine a Scam Email

Unexpected Attachments

Inconsistent URLs

Action Required:
Requests to
Update
Information

Misspellings and Poor Grammar

Something's "Off"

W-2 Form Request

An Email from the CEO

You've Won a Contest A Tone of Desperation





Keep Yourself Protected Online

- Use a virtual private network (VPN), a protected network connection when online to add an extra layer of protection, and avoid using public Wi-Fi when possible.
- Be on the look out for "https" in website addresses, ensuring that the "s" is there will increase encryption and therefore security when sending credit card information.
- Be careful with what you share via social media or email and cross check any claims made.
- Keep virus protections updated and be sure to use strong passwords for each account.

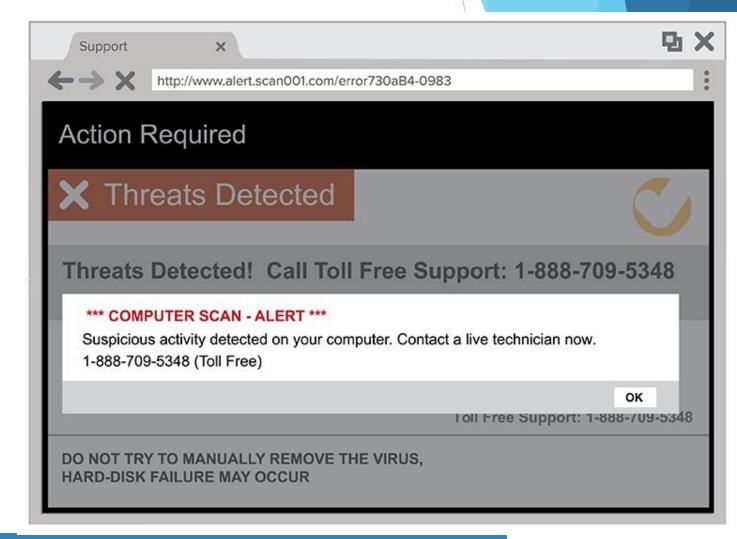






Tech Support Scams

- Legitimate tech companies won't contact you by phone, email or text message to tell you there's a problem with your computer.
- If you get this kind of pop-up window on your computer, don't call the number. Real security warnings and messages will never ask you to call a phone number.







Caregiver Fraud Defined

- California Penal Code Section 368 defines a caregiver as "Any person who has the care, custody or control of, or who stands in a position of trust with an elder or dependent adult."
- Caregiver fraud occurs when that person designated as a caregiver physically or financially abuses the dependent.
- This form of abuse usually begins with deception about the true identity or qualification of the caregiver.

- Caregiver fraud comes in many forms and includes acts of:
 - Physical harm or suffering
 - Endangerment
 - Forgery
 - Identity theft
 - Embezzlement
 - Theft





Six Types of Elder Abuse Exist

Physical

Hitting, kicking, pushing, slapping, burning, or force causing injury

Sexual

Engaging in sexual act without consent

Emotional

Harming self-worth or emotional well-being, name calling, & scaring

Neglect

Failing to meet basic needs like food, housing, clothing, & medical care

Abandonment

Leaving elder alone or no longer providing care

Financial

Illegally misusing an elder's money, property, or assets

Learn how signs of elder abuse differ from normal aging to prevent elder abuse before it happens.







KNOW THE SIGNS OF ABUSE

Physical Signs of Elder Abuse



Dehydration or unusual weight loss



Missing daily living aids



ing Unexplained injuries, bruises, cuts, or sores



Unsanitary living conditions and poor hygiene



Unattended medical needs

Emotional/Behavioral Signs of Elder Abuse



Increased fear or anxiety



Isolation from friends or family



Unusual changes in behavior or sleep



Withdrawal from normal activities

To learn more, visit ncea.acl.gov

Financial Signs of Elder Abuse



Fraudulent signatures on financial documents



Unpaid bills



Unusual or sudden changes in spending patterns, will, or other financial documents

To learn more, visit ncea.acl.gov

To learn more, visit ncea.acl.gov





How to Report Fraud & Scams

- Report suspicious activity at 562-435-6711
- Or dial 9-1-1 for emergencies

Long Beach Police Department (LBPD)



- Report fraud & identity theft online at <u>ftc.gov</u>
- Or call 877-FTC-HELP

Federal Trade
Commission (FTC)



- Report internetbased fraud at <u>ic3.gov</u>
- Submit a tip at tips.fbi.gov

Federal Bureau of Investigations (FBI)



 Report mail fraud, mail theft, & identity theft at

uspis.gov/report

United States
Postal Inspection
Service (USPIS)







What We've Learned Today

- Monitor and protect your personal information
- Be careful with what you share, especially online or over the phone
- Cross check any claims made with primary, trusted sources or people
- Start a conversation with your loved ones
- ► **Get more information** from ftc.gov/PassItOn





Need Assistance? We Can Help!

What We Do:

- Elder Fraud & Abuse Victim Assistance
- Peer Support & Resource Referrals
- Vacationing Home Security Checks
- Graffiti & Dumped Item Reporting
- Crime Prevention & Awareness Presentations
- Handicapped Parking Warnings & Citations
- Limited Safety Patrols
- Special Event Assistance









Senior Police Partners—Contact Us!

Summer Smith, Volunteer Coordinator

For more info, visit: https://bit.ly/lbpd-spp

<u>SPP@longbeach.gov</u> | **€** 562-570-7212