Seal Beach Police Department
911 Seal Beach Boulevard, Seal Beach, CA 90740

June 14, 2023

FOR IMMEDIATE RELEASE

Contact: Lieutenant Julia Clasby
(562) 799-4100 ext. 1161
jclasby@sealbeachca.gov

Scam & Fraud Prevention Tips

SEAL BEACH, CA — The Seal Beach Police Department has realized a significant uptick in financial “scam” and “fraud” crimes, primarily targeted at our senior citizen population. The Seal Beach Police Department realizes the best way to stop these types of scams is to build awareness and provide preventative suggestions to thwart these crimes before they occur. Therefore, we have compiled a host of preventative measures to unveil mechanisms used by scammers and recommendations on how to best combat being victimized.

Scammers create many scenarios to facilitate their crimes, including threats of violence to pressure their victims into feeling hopeless, intimidated, and having no recourse but to send money. Phone calls, text messages, emails and computer pop-up ads via the internet and social media are the most common types of mediums used by perpetrators. These methods are preferred due to the fact victims can be contacted worldwide through these devices. The following is a compilation of the most common types of mechanisms used by fraudsters; however, this list is not exhaustive.

The Federal Communications Commission (FCC) estimates there are nearly 2.4 billion robocalls made each month. Robocalls often use spoofed area codes to appear like they are calling from the victim’s local area or with the caller ID of a government agency. Typically, an automated message will then inform the victim that they owe money or need to take immediate action on an issue.

Family imposter scams
Fraudsters may pose as officials from government agencies, banks, friends or family members to trick people into revealing bank account numbers, passwords and other personal data.

In family imposter scams, fraudsters pose as a loved one either by creating an online profile that looks like them or hacking personal emails or social media accounts. They will often claim an emergency has left them in desperate need of money and request an immediate transfer of funds.

If a family member is asking you to send them money online, it's important to vet the person you're talking to and ask them questions only your loved one would know. It's also important to avoid sending money immediately. Scammers bank on your fear and anxiety, but if you take a moment to call your relative directly, you can confirm if they really need your help.

Social Security Administration imposter scams
Social Security imposters may tell victims that their SSN has been linked to criminal activity and/or suspended. The scammer will claim they can reactivate the number once the victim confirms their SSN. Other Social Security scams may tell victims their benefits are eligible for an increase and request that they confirm their name, date of birth and SSN. Both approaches are ploys to gain access to personal information that can be used to access private accounts and personal finances.

Actual representatives from the Social Security Administration won't ask for your SSN over the phone, nor will they initiate contact if you haven't recently been in touch with them. Warnings of arrest, the suspension of your Social Security number or the loss of benefits are also signs that the notice is a scam.

Internal Revenue Service imposter scams
Another one of the most prominent government scams is IRS impersonation. This type of scam usually involves calling victims directly and telling them they owe taxes that, if not paid, could lead to their arrest or other legal action. The scammer's goal is to intimidate victims into immediately sending the requested money or providing personal information, like bank account or Social Security numbers.
The Department of the Treasury recommends immediately hanging up if you receive a phone call matching these characteristics. If there's an issue with your taxes, the IRS

will typically send a notice in the mail first. The IRS also will never ask for personal financial information like PINs, passwords, or credit card numbers.

Lottery and Sweepstake Imposter Scams

In 2020, the FTC received over 116,000 reports about sweepstakes- and lottery-based scams. Victims of all ages lost a total of at least $166 million, with a median loss of $1,000. According to the Better Business Bureau (BBB), this type of scam usually targets older people.

Sweepstakes fraudsters often make contact through mail, phone calls, email, or social media. Social media now accounts for one-third of reported lottery scams, according to the Better Business Bureau. In the typical pattern of a sweepstakes fraud, the victim is congratulated on winning a massive amount of money. In order to receive it, though, they must pay a processing fee or tax. The amount the scammer asks for will vary, but if someone pays it, they will usually call asking for more money in order to deliver the prize to them.

True sweepstakes generally state, “no purchase necessary,” and winners should never be asked to send money to claim their prize. Legitimate lotteries like Mega Millions or Powerball sell tickets, but they will never charge participants money to receive their prizes.

Computer Tech Support/Virus Imposter Scams

Tech support scammers tell victims their computers have problems or viruses that they can help resolve. They then make money by asking victims to pay for services that aren’t needed. In 2019, tech support scammers stole $24 million from victims over 60. Sometimes, these scammers call people directly, warning about “computer problems,” but the most common way tech support scammers connect with victims is online.

On certain websites, pop-up warnings may appear, warning users of a virus or security issue on their computers. Though the message sounds urgent and may use official-looking logos, it’s just a way to trick the user into making contact and sending money. Often, tech scammers claim they are from a well-known company like Microsoft or Apple. However, major tech companies say they do not contact customers about these issues. When these pop-ups appear, simply close out the tab and ignore the warning.

Scammers may also ask for remote access to your computer. While legitimate computer care companies may do this to resolve technical issues, you shouldn't grant remote access to your computer to anyone that you haven't vetted whoever's on the other end. Fraudsters are always finding new methods to trick people into giving them money. Whether or not the method is listed here, it's important to be skeptical of anyone who is asking for advance or immediate payment, especially via gift card or wire transfer, and bit coin, money transfer, or cryptocurrency. Resist the pressure to act quickly.

Scammers create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one. When in doubt, don't send any of the requested money, and talk to someone you trust about the potential scammer who contacted you.

Bullet points to remember - PROTECT YOURSELF

- Nobody legit will ever (EVER) tell you to pay by gift card.
- No government agency will ever call/email/text to ask you for money, your Social Security, bank account, or credit card number.
- Recognize scam attempts and end all communication with the perpetrator.
- Search online for the contact information (name, email, phone number, addresses) and the proposed offer. Other people have likely posted information online about individuals and businesses trying to run scams.
- Be cautious of unsolicited phone calls, mailings, and door-to-door services offers.
- Never give or send any personally identifiable information, money, jewelry, gift cards, checks, or wire information to unverified people or businesses.
- Make sure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls.
- Disconnect from the internet and shut down your device if you see a pop-up message or locked screen.
- Be careful what you download. Never open an email attachment from someone you do not know and be wary of email attachments forwarded to you.

For more information about scams, go to the Federal Trade Commission website at https://www.consumer.ftc.gov/. Report any suspected telephone scams to the Seal Beach Police Department at (562) 799-4100.

####

FEDERAL TRADE COMMISSION

A Scammy Snapshot of 2022

(based on reports to Consumer Sentinel)

#FTCTopFrauds
ftc.gov/data
ReportFraud.ftc.gov

Top Frauds

1. Imposters
2. Online shopping
3. Prizes, sweepstakes, lotteries
4. Investments
5. Business and job opportunities

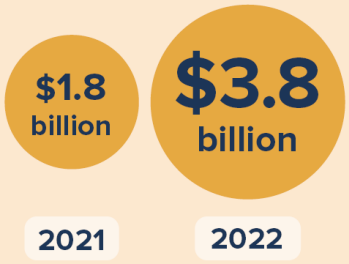
2.4 million fraud reports

$8.8 billion reported lost

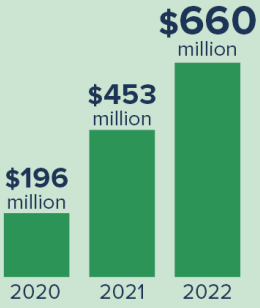
The number of reports is down.
The amount lost is up.

(2021: 2.9 million fraud reports, $6.1 billion lost)

Losses to investment scams **more than doubled.**



Losses to business imposters soared.



Scammers contacting people on social or by phone led to big losses

$1.2 billion total lost

Social media: Highest **overall** reported losses

$1,400 median loss

Phone calls: Highest **per person** reported losses