TOOLS FOR LIFE: Fraud and Scams During COVID-19

Financial scams and fraud have been on the rise lately, when COVID-19 has forced us to stay home. Everyone is at risk of being a victim. To help protect you during this vulnerable time, JFS invited Ken Jonah to lead a Zoom Discussion Group on this topic. For the last 5 years, Ken has been a volunteer for the Fresno Police Department's Northeast District's Citizens on Patrol Volunteer Unit. Formerly, Ken was a police commissioner in Contra Costa County for 12 years.

Each year, millions of Americans of all ages fall victim to some type of financial fraud, racking up more than $3 billion in losses annually. Anyone who has a phone or a computer is at risk of a scam, which Ken defined as "an attempt to deceive which involves a financial transaction for the purpose of [the criminal's] financial gain." Scammers prey on the number one emotion of their victims—fear—as they attempt to gain a victim's trust by communicating with the victim in-person/knock on the door, via telephone/robo-calls, via mail/email, or as pop-ups on computers or devices.

Common Methods of Scams and Fraud:

- ***Telephone Spoofing/Robo-Calls*: According to Ken, criminals are "so sophisticated that they can create a [telephone] number that looks exactly like yours [or someone you know], including the area code and prefix, and call you all day long."**
- ***Family Medical-Emergency Scam*: Per Ken, "Scammers go online and browse Facebook to see whose doing what." For example, I might post an update that I am going to Dallas. A scammer then finds this, waits about a week, then calls my husband and says, "This is the Dallas Police Department. Your wife's been in an accident. We got her phone from the car to call you and let you know that she's going into surgery right now. This particular hospital needs a deposit of $5,000 prior to beginning the surgery." The scammer then insists that payment of $5,000 be in the form of a gift card to Target or some other major retailer. Red flag: Hospitals do not accept retail gift cards as a form of payment.**
- ***IRS/DMV/Government-Impersonation Scam*: Perpetrators pose as government employees and threaten to arrest or prosecute victims unless the victim agrees to provide funds or other payments. Scammers pose as the IRS or DMV, telling the victim that they have an unpaid, overdue bill. They threaten that, unless the bill is paid, in the form of a gift card, they will send law enforcement to the victim's home and make an arrest or revoke the victim's driver license. Per Ken, "The biggest red flag is that government agencies don't call, and they don't ask people to pay with a gift card."**
- ***Romance Scam*: Perpetrators pose as interested romantic partners through dating websites to capitalize on their victims' desire to find companions. In one case, the scammer posed as a beautiful lady. After a few exchanges, the scammer sweet-talked the victim by saying she'd like to meet but had no money for airline tickets. So the victim sent the scammer money for**

airline tickets. The scammer then claimed she's run into another problem—her passport needs to be renewed and, in her country, it costs $10,000 to renew a passport. The victim then sent her money to renew her passport. Two weeks later, the scammer requested additional money to speed up the 1-year, passport-renewal process. Ultimately, the victim lost over $420,000—as well as his home, pension, and car in the process. Don't get scammed: Resist the pressure to act quickly. Perpetrators create a sense of urgency to produce fear and lure victims into immediate action. If a romance blossoms too quickly or a romantic partner requests money or your personal information, it's a scam.

- ***Grandparent Scam:*** **Perpetrators pose as a relative—usually a child or grandchild—claiming to be in immediate, dire financial need, such as bail money, as they plead with the victim to not discuss the arrest/bail with anyone. Such calls typically come late at night. The scammer insists the victim send the "bail money" in the form of a gift card. Don't get scammed: Insist that the caller give you a telephone number and tell them you'll call them back. Or request they call you back, all while you call the child's parent or the child to verify.**
- ***Sweepstakes/Charity/Lottery Scam:*** **Perpetrators claim to work for legitimate, charitable organizations to gain victims' trust. Or they claim their targets have won a lottery or sweepstakes, which the victim can collect for a "fee." If you did not enter the contest or sweepstakes, it's a scam.**
- ***Internet/Sale Scam:*** **Seller beware—scammers scour ads posted by victims who are trying to sell items online (e.g., Craig's List or Ebay). Say I post an ad to sell my TV for $500, but I receive a payment/check from a scammer for $2500. Scammer then tells me they've made a mistake, as they purchased two items on the same day and accidentally sent me the payment that was meant for the other seller/item. The scammer then asks me to send them their $2,000 overpayment and oftentimes even insists that, for my trouble, a payment for $1900 will suffice. While I am refunding them their overpayment, the scammer's $2500 payment to me bounces or is no good. I lose $1900 and am stuck with the TV I was trying to sell in the first place.**
- ***Tech-Support Scam:*** **Perpetrators pose as technology support reps and offer to fix non-existent computer issues—gaining remote access to victims' devices and, thus, their sensitive information. This is typically done via computer pop-up messages, warning the victim that their computer is infected with a virus and offering to repair it by requesting access to the victim's computer. By gaining access, the scammer is also able to access to the victim's personal and financial information, including passwords. Be suspicious of any unsolicited "computer security experts" repair scams. Don't click on any unknown links, visit any unknown sites, or install software—these are regularly used by perpetrators to spread malicious software. If you receive a pop-up or locked screen on your device, immediately disconnect from the Internet and shut down the affected device. To avoid accidental clicks on or within a pop-up, enable pop-up blockers.**

- ***Prescription-Drug Scams*: Prescription-drug/Medicare scams tend to target elderly victims. Discounted medications may appear legitimate, but the medications are often counterfeit, diluted imitations that come from other countries, such as Canada or Russia.**
- ***Home-Repair Scam:* Perpetrators appear in person and charge homeowners in advance for home improvement services that the scammers never provide.**
- ***TV/Radio Scam*: Perpetrators target potential victims using illegitimate advertisements about legitimate services, such as reverse mortgages or credit repair.**
- ***Family/Caregiver Scam:* Perpetrators can be relatives or acquaintances of victims, especially elderly victims, and take advantage of them or get their money. Once the criminal gets their hands on a victim's money, that money is typically gone and untraceable.**

Ways to Protect Yourself:

- **Call the police immediately if you feel there is a danger to yourself or a loved one.**
- **Be cautious of unsolicited phone calls, mailings, and door-to-door services/offers. If you don't recognize the number, don't answer. If it's someone you know, the person will likely leave you a voicemail. Ken shared his clever method of thwarting calls from unknown numbers—he answers the call and says, "Sheriff's Department, fraud division," or "Police department, fraud desk."**
- **Never give or send any personally identifiable information, money, jewelry, gift cards, checks, wire information, or funds—to unknown or unverified persons or businesses.**
- **Ensure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls.**
- **Do not open any emails or click on attachments you do not recognize and avoid suspicious websites. Beware of some emails that deceptively appear to be from someone you know or someone in your contacts list. Before opening an email that seems odd or suspect, reach out to the contact and ask if the contact sent you an email.**
- **If a perpetrator gains access to a device or an account, take precautions to protect your identity, immediately contact your financial institutions to place protections on your accounts, and monitor your accounts and personal information for suspicious activity.**
- **If you've experienced a scam, particularly elder-abuse related, you can reach out to Detective Doug Reese, Elder Abuse Division, Fresno Police Department—call (559) 621-6318 or email Doug.Reese@Fresno.gov**
- **If you believe you have been the victim of an Internet crime, or if you want to file on behalf of another person you believe has been such a victim, you can file a complaint online with the FBI's Internet Crime Complaint Center (IC3) by visiting https://www.ic3.gov/Home/FileComplaint**
- **When reporting a scam—regardless of dollar amount—be as descriptive as possible in the complaint by including dates the perpetrator had contact with you, the methods of**

communication, names of the perpetrator or company, phone numbers, email addresses, mailing addresses, websites, method of payment, account names and numbers, financial institutions to which you sent funds (including wire transfers and prepaid card payments), descriptions of interactions with the perpetrator, and any instructions you were given.

- **Keep all original documentation, emails, faxes, and logs of all communications.**

Fraud and scams happen quickly and often. Be prepared, be aware, be suspicious, but don't be a victim.