SENIOR SCAMS: DETECTION AND PREVENTION: Kris R. Ludwigsen, PhD

A scam is a transaction involving deception that benefits one party at the expense of the other. Scams abound like cold germs in winter; we can take protective measures (hand washing) but the odds are that we'll be exposed and may succumb at some point. Seniors are prime targets based on: (1) specific areas of naiveté, (2) vulnerability/ availability, and (3) access to affluence.

> Naiveté /blind spots re your computer, car, home operating systems, etc., when things go awry in systems that are too complicated for the average user to understand. We have a functional but not a systemic understanding of what we rely on; and we live in an increasingly complex, interdependent society.
>
> Vulnerability /availability: An immediate (heater broken) or ongoing need (loneliness); traveling solo; being sick or recovering from surgery and needing help with home maintenance or repairs. We're most susceptible to fraud within three years of a trauma stressful event, e.g., deaths, illness, or a move to a new residence, per AARP. And we seniors are vulnerable to cognitive decline: Like swiss cheese our memory develops holes starting at age 50; ongoing problems take up our concentration, and our ability to multitask, to process new or complex information in order to make decisions slows down with aging.
>
> Financial resources: IRAs, investments, nest eggs, etc., designated for emergencies and retirement, or the ability to borrow large amounts of money.

Per AARP about 1/3 of all scam victims are 65 or older but are only 1/8 of the US population. Other scams target specific religious, ethnic, or sexual "affinity groups," e.g., Veterans, or survivors of the recently deceased.

Types of scams

> Financial investments (Bernie Madoff): Free-lunch seminars hawking dubious products; Telemarketers offering "no-risk" investments; financial/fiduciary abuses
>
> Homeowner scams: Dubious moving company estimates; Unnecessary repairs, replacements or renovations. Workers claiming to be from your HOA or who "upsell" more repairs until you're bled dry.
>
> Health care: Callers asking for your Medicare/SSN number, claiming that Medicare is issuing new cards, entitlements or refunds that require "verifying" your SSN. Callers offering free/discounted medical supplies for diabetes, heart disease, etc., who need your age, SSN, MD's name and phone number (a red herring?). In medical identity theft imposters obtain health care services under your name. Bogus contracts for nonmedical homecare as a substitute for (more expensive) long-term care insurance.
>
> Identity thieves engage in dumpster diving, steal wallets or purses or skim credit/debit cards via special devices. They go "phishing" by e-mail to obtain your personal info via spam or pop-

up messages or through your iPhone or send in a "change of address" form to the USPS. They can follow mail delivery vans and scour your mailbox for new checks, tax info, or bank/credit card statements. They may steal personal records from employers or others with access to the information.

Travel/ vacation scams in winning a "free vacation," rentals, time shares difficult to get out of; other property or land purchase scams (swamp land in Florida years ago).

Lotteries and sweepstakes that require a fee to claim nonexistent prizes (cars) or cash. If you send the ($39.95) fee you're on the sucker list and ripe for future come-ons by mail, phone or Internet. Some mail a phony "partial-payment" check under $5000 to deposit to further lure you in. (By law banks must make the amount available in five days but are actually fronting the money until the check clears.)

Sympathy appeals: Someone you know is in trouble and needs money, e.g., your grandkids have been kidnapped (a child is screaming in the background) or are in a Mexican jail for drug use (college students); Friends just had their wallet stolen in a foreign country and are stranded; Widows or widowers are begged to send funds via via wire transfer to "catfishing" online friends with a "temporary" or dire need who then disappear or are declared dead. (Where's the obituary?)

Unnecessary/protection "services" for your computer, e.g., that require remote access (may lead to identity theft), car, home maintenance and repair. Scammers then "discover" additional problems. "Security checks" (AmEx); "account billing info" (Netflix)

Mode of contact

Via computer: e.g., *Microsoft* (blaring, but no logo) has identified a major problem and has frozen your computer; call this toll-free number to authorize remote access to "fix" it. Scammers then install malware, charge you to remove it, and offer a monthly "protection service" for $24.99. E-mails from *B of* A warn of "suspicious activity" in your account. *Client Care Experts* in Florida (a senior haven) installed phony pop-up warnings on computers. A Microsoft study found that 4/5 Americans had been hit with tech support scams.

EBay sellers post a photo of the quality/name-brand merchandise, then ship the knockoff. Online crooks steal the logos of legitimate companies to promote "free giveaways," then lure you into malware-infected links that infect your computer.

*AmEx*" (with official blue logo) or your bank needs more personal data to "update" their records (= *artisanal spam* with personalized traps); *Ransomware* can freeze your electronic records; *FedEx* has a delivery for you; *FaceBook* contains phony apps and connections to malware-infected links. Scammers harvest information for names of grandkids, when you'll be on vacation, etc.

E-mails claiming to be from the *IRS* aim to steal your money and/or identity. Identity thieves will file taxes early after obtaining your SSN. They collect personal data from *LinkedIn* and other social networking sites, obituaries, www.ancestry.com. Bogus e-mails from the CEO or HR asking corporate employees for log-in credentials. Internet sites can masquerade as the DMV, etc., to charge more for renewing online; "*Yahoo*" threatens to cancel your account; "Microsoft" voicemails claim that your services are about to be canceled. *Smartphones* can be hacked; malevolent links sprout on Twitter.

Via telephone: The IRS is filing a lawsuit against you--call this number (or the CC Sheriff's office) immediately; "There's a warrant for your arrest." Microsoft/Windows will eliminate your services by 3:00 pm unless you call; PGE will cut off your power tomorrow if you don't pay the caller now by credit card. Texts claim that a friend is stranded abroad and desperately needs you to wire funds--which cannot be reclaimed. Threats to arrive at your door to haul you off to jail. Caller IDs can be manipulated via "spoofing" products or Internet-based phone lines with legitimate- appearing numbers/organizations. (The FBI nabbed a ring of scammers operating out of India.) And some callers sound friendly and personable to lure you into their scam.

Via US mail: Flyers offering a "free"/low cost (heating system) inspection or other services; "Porch pirates" and mailbox trawlers stealing mail/checks for identity theft, especially by drug users. Bogus solicitations for reverse mortgages or offers to take over house payments (= home stealing).

Door to door: Offering home inspection, installation or repairs, pest control ("Working on your neighbor's home, we noticed bugs in yours."); students selling overpriced (or unordered) subscriptions to "raise money for tuition."

Personal: Using your church or social groups or other relationships to create or play on your trust for financial gain.

Conclusion: Any new or established form of communication can be an avenue for scammers to operate. Advances in technology have made it easier to cast a broader net.

Tactics

Inducing fear or panic (IRS, kidnapping). Under anxiety behavior tends to stereotype and precludes our ability to think rationally or find creative alternatives; the brain's amygdala mediating emotion then dominates the frontal cortex. We all have blind spots and triggers that create psychological vulnerability. Predators and scammers are adept at identifying their best prospects and knowing what approach will be most convincing; that's their business and they are becoming more sophisticated.

Flattery, soft-soaping: "We wish all our customers were like you." Aligning or identifying with you (e.g., as a military vet); taking a personal interest in you. Being at hand, affable and able.

Pseudocredibility/reassurance: We're Diamond Certified and on Angie's List; We're A+ rated with the Better Business Bureau; Come-ons: We don't charge for diagnostic work; We drug-test all our employees; We have the ultimate solution to your problem.

Bait and switch: You need a more costly product or service; We've found additional work that needs to be done on this repair (now that it's underway). Can apply to unnecessary or risky proposed medical or dental procedures.

Wearing you down with pressure tactics. Since mental alertness peaks midmorning and tapers off after 2:00 pm, scammers often contact you late in the day (or very early in the morning). Isolating you at the airport; double-teaming the mark.

Orchestrating a series of "yes" answers to build momentum and then sell you extras you don't need after wearing you down. (What are the statistics in extended warranties?)

Plausible rationalizations about what's wrong with your computer, car, heating system, etc., after sizing up your lack of knowledge.

Counting on poor memory to obtain multiple payments for services, magazine subscriptions, etc. (One senior was paid up for *People* magazine through 2022).

Offering a "great deal"/time-limited promotion too good to pass up (for financial gain, home maintenance, medical equipment or services)

Financial persuasion tactics include: dangling the prospect of wealth based on a limited window of opportunity; claiming special credentials or experience, e.g., as part of a reputable firm or special group; offering small favors to obligate you; claiming social consensus through people you know and/or respect.

Psychological Factors: If this offer is the "answer to your problems or prayers" or "too good to be true," think twice. Under the right circumstances anyone is vulnerable, regardless of age/ gender/ IQ/ education/ socioeconomic status/ position/ or financial experience, especially if there's a crying need (real or bogus) and a credible rationalization.

Under pressure we can cave in because we want to do the right thing for peace of mind or to do what's expected of us. Seniors and people of faith can be too cooperative, polite, loyal or trusting. We may want to see ourselves as responsible, intelligent and competent but can fear we don't know enough re technology, etc. We want to comply, to feel needed or important, to belong, especially if friends, peers, or others we respect are involved.

Scammers play on how women are socialized and can sense how you want to view yourself, in order to offer specific validation and reassurance. Per AARP seniors can be counted on to respond to appeals to aid for veterans, needy or sick children or animals, disaster victims, etc.

Who are the perpetrators?

1. Commercial enterprises that misrepresent what they're offering or upsell goods or services you don't need (extended warranties); who bill you for home or auto repairs that are promised but not done or done in a substandard, shoddy way, who slip in hidden fees (as in paying bills by telephone vs. check). "Free-trials" for products may be offered by scammer vendors and their endorsements may be fake as well.

2. Fly-by-night operations (IRS scares) that continually change their (disposable and dedicated) cell phone numbers and so are difficult to track down.

3. Cons who rely on rely on financial or "sweetheart scams" to make a living (the online beau who disappeared after taking the widow's money.) Grandparent scams often operate out of Canada with numbers easily disguised or difficult to track. They've done their homework on your family via Facebook or obituaries, etc., and pose as police officers, attorneys, afflicted children and/or hospital aides.

4. Opportunists, e.g., at the airport or the car repair shop. Some obituary trawlers call spouses, children or siblings to claim that survivors must repay the deceased's debts. They may alert you to (fictititious) life insurance policies that require final payments, tax premiums, handling fees, etc., before collecting, or may even pose as clairvoyants with a message from the beyond for the grieving.

5. "Entrepreneurs" offering special services (door-to-door, etc.); Some scammers have a natural talent to manipulate (Frank Abagnale in "Catch me if you can") or view it as a game to con the mark.

6. Sociopaths and psychopaths believe their own lies and lack a conscience so they come across as sincere in person with no "tells." The scam artist is often charming and personable, attractive and well-groomed. He or she knows how to appear knowledgeable, successful, and credible. Cons ask questions to build rapport and to customize their pitch. The "con" stands for the "confidence" they inspire. When confronted they claim, "I got my own mother into this investment--I didn't know," to neutralize accusers/friends.

7. "Stealth scammers" research unoccupied (or occupied) properties at the City Hall; then use property transfer forms from Staples, etc., to forge the seller's signature before filing this paperwork with the city/county recorder's office. (investigated by DA Kamala Harris in San Francisco). Some forge fake IDs to steal the real homeowner's identity. Hijacked homes can then be sold for a fraction of their worth or used as collateral to obtain new loans. Lenders favor homeowners with no existing mortgages and many seniors have paid off their mortgages.

Others use special software to collect personal details from LinkedIn and other social networking sites. They send malware-infected links in e-mails ostensibly from Facebook friends. By clicking on the link, every keystroke is sent to the crook, including online accounts where you enter your name and password.

Scammers can present as personable young men or women who offer to help, who appear innocuous and trustworthy. Some appear with an "official" badge/ID or (rented) uniform, etc., to enhance their credibility.

Others try to get you to feel sorry for them to give them yardwork or donate to a bogus cause or charity (at the grocery store) that you can't take time to check out. Scam artists are sophisticated sales psychologists and many people are trained in the business of persuasion or of selling something tangible (miracle weight loss products) or intangible (psychotherapy, spiritual healing), legitimate or not. We need to scrutinize the motives and methods behind these efforts to persuade.

Psychological research shows that we make up our minds within 3 - 5 minutes on whether we like the other based primarily on nonverbal cues, including clothing and facial expression. Scam artists are good actors and know how to appear sincere (using mirroring, etc.). Neurological changes with age can cloud our ability to recognize facial expressions that signal deceit. Newer scams can be ingenious and creative, thereby harder to evaluate; and there's a scam hatched every second, a plethora online per AARP.

Motivations: Scammers are aiming for an entitled lifestyle of luxury and status or to fund a drug habit. Some are gratifying power or ego needs and/or are naturally good at manipulation. They do their utmost to build their credibility, play to your vulnerability and prey on your trust, naiveté and blind spots as well as on existing anxiety and fears. Con artists fine-tune their methods in times of crisis (financial or natural disasters) knowing that victims are feeling increasingly desperate; they use every ploy or trick in the book.

How can you protect yourself? Deception is an omnipresent part of life and we can fail to recognize the obvious or spot the red flags; but forewarned is forearmed. You can increase your awareness and decrease your exposure and your vulnerability via these approaches designed to "tase" your adversary.

1. Take time to evaluate the offer rationally. (I need to think it over, talk to my spouse/ partner, brother, son, brother-in-law, attorney, financial advisor, etc.) Google or otherwise check out those offering that good deal. Be skeptical and ask for an objective evaluation on the proposal from a disinterested and knowledgeable party.

2. Avoid making decisions based on fear, anxiety or panic or other strong emotions, especially in high pressure situations; stay calm and breathe. If swept up in optimism or enthusiasm ask yourself what's the downside of the situation in cost, commitment, etc. What's your gut/intuitive feeling?

3. Identify your needs, hopes and fears in the matter. "Sweetheart" scams play on the yearning for a life partner or an intimate connection.

4. Remove yourself from the pressure, e.g., escape to the ladies' restroom at the airport or claim a migraine. Avoid answering unknown landline or cell phone callers or pressing a button to "opt out" and assume that any threats are bogus.

5. Be aware: Read and research online, etc., to become knowledgeable. The AARP *Bulletin* (e.g., re SmartPhones), the *EastBay Times* and *Rossmoor News* run exposés on scams. Know that the IRS does not contact via telephone, nor Microsoft by computer.

6. Get referrals of reputable providers from friends and neighbors, news sources (Diamond Certified businesses, Best of the East Bay readers'choice awards) or online (Better Business Bureau, Home Advisor, Angie's List) although this is not foolproof.

7. Share information and experiences. Don't be deterred by shame or chagrin; we're all vulnerable at some time to a scam or con artist. Vulnerability is our human condition per Buddhism.

8. Don't send money to online "friends" or lovers or donate to persons or charities you don't know well, no matter how strong the appeal. Check out the charity/requestor. Call or do a brief online search to verify claims to be the attorney/firm, police station/ hospital/sheriff's office. Call a family member to get an update on your grandchild before wiring money.

9. Know your rights: The Federal Trade Commission/FTC allows you three business days (72 hours, including Saturdays) to cancel a contract over $25 without explanation; you can stop payment on your (deposit) check as well.

10. Be skeptical about unsolicited offers of services by telephone, US mail or e-mail. Offers of free/low cost medical supplies aim to extract personal information (SSNs) from Medicare members. Computer hackers are ever bolder and more sophisticated; the Internet offers a much broader scope for a low investment of energy.

11. Prevent identity theft by using a lock on your home mailbox and deposit mail in the USPS mailboxes or slots close to collection times; use a confetti shredder for paperwork with your name, DOB, SSN, address; use online banking vs. mailed statements; change your passwords or use a password manager; download HTTPS Everywhere to encrypt Internet communications; use a gel pen on checks.

12. Obtain and monitor your free credit report; use www.lifelock.com to check credit; freeze your credit so no one else can open an account; use a VPN service with free Wi-Fi; monitor all financial statements; use a password with upper and lower case letters plus numbers and symbols, and an unusual pin (no DOB).

13. Don't let strangers into your home especially in pairs; one can distract you while the other steals. Keep tabs on neighbors' homes when they're away and ask that they do the same for you.

14. Don't set your residence as "Home" on your GPS; parking attendants can download keyless entry systems to syouartphones. Don't keep auto registration, debit card, etc., receipts in your glove box. Dispose of address labels so as to foil dumpster divers.

15. When registering on a website or purchasing online, set up another (free) e-mail account for purchase confirmations or registration numbers.

16. Confirm property records with the local deed recorder or register's office to ensure that all documents and signatures are legitimate. Check the issuer on any new payment book or other notices on loans you haven't initiated.

17. Be stingy with personal information on social media, random surveys, product registration forms, etc. On obituaries avoid giving information on the departed and such as full name, address, birthdate, mother's maiden name, birthplace, hobbies and surviving family members.

18. Stay informed via local resources, e.g., Nextdoor.com, friends and family, local news sources, affinity groups, and the bimonthly AARP *Bulletin*.

Senor Scam Resources

"Frauds, Scams, Rip-Offs," AARP.org/bulletin, April 2017, pp. 14-16.
*Scam Alert: An AARP Guide*, July 2017, ISBN: 978-0-9971287-1-0
Sid Kirchheimer, *Scam-Proof Your Life*, AARP Books/Sterling; Contact at asksid@aarp.org
*Fraud Fighter* hotline: 800/ 646-2283 or 877/908-3360; *Protecting Yourself Online for Dummies*; www.aarp.org/fraudwatchnetwork

*Protect Yourself from Fraud*. California Department of Business Oversight. For copies call 1-866-275-2677 or e-mail publications@dbo.ca.gov. To file complaints on brokers, investment advisors and financial institutions, call 866/275-2677 or download forms from www.dbo.ca.gov

SEC: www.sec.gov/investor/seniors.shtml

Affinity Fraud: www.sec.gov/complaint/select.shtml.
Protecting Senior Investors: www.sec.gov/spotlight/seniors/seniors_summit.htm

California Dept. of Consumer Affairs for complaints: 800/952-5210, www.dca.ca.gov
California Contractors State Licensing Board for complaints: 800/321-2752, www.cslb.ca.gov
www.CheckTheLicenseFirst.com; www.SeniorScamStopper.com

US Postal Inspection Service 1-877/ 876-2455 to report phishing ploys, mail fraud, theft resulting in financial losses, and scams. In Oakland, contact Inspector Albert Rodriguez, for documents, forged checks, etc., supporting reported financial crimes at Fax: 510/622-7413.

Federal Bureau of Investigation: www.fbi.gov

Deter-Detect-Defend Avoid ID Theft: www.ftc.gov/idtheft, 1-877-438-4338 (1-877-ID THEFT) Federal Trade Commission complaints: www.ftccomplaintassistant.gov 1-877/ 382-4357.
www.OnguardOnline.gov

Charity scams: www.charitynavigator.com. For free credit reports: www.CreditKarma.com and www.CreditSesame.com. For black market use of your SSN and any three credit cards: www.TrustedID.com/idsafe/identity-protection; Bank of America: abuse@bankofamerica.com

Medical Board complaints: 800/633-2322, www.mbc.ca.gov
MediCal abuse: 800/722-0432, www.ag.ca.gov Medicare: 800/633-4227 (TTY: 877/486-2048)
HMO complaints: 888/466-2219, www.dmhc.ca.gov
Veterans Affairs complaints re providers: 800/ 736-7401, www.dir.ca.gov/dwc

Adult Protective Services re fiduciary or physical abuse by a caretaker, relative, neighbor, friend. (Elder abuse is "notoriously underreported" since the senior is in a dependency relationship to the abuser); In immediate need call 911 or the police); In Contra Costa call 1-877/ 839-4347 via landline, or 925/ 602-4177. In California call 800/722-0432, www.ag.ca.gov Attorneys are available via The Family Justice Center in Concord (521-6366) in Todos Santos Plaza

**(for inside back cover)**

[Photo] Dr. Kris R. Ludwigsen is a retired Diablo Valley Kaiser clinical psychologist and a former USAF and USAFR clinical psychologist whose recent presentations have focused on "Psychological Factors in Senior Scams" designed to promote awareness, prevention and recovery based on her firsthand experience. She is a Fellow of the American Psychological Association and a senior member of the Contra Costa Psychological Association.