Stanford Center on Longevity

A **TOOLKIT** SERIES BRIEF

AVOIDING FRAUD 101

Default Behaviors to Resist Fraud

Marti DeLiema
Postdoctoral Scholar
Financial Security Division
Stanford Center on Longevity

STANFORD CENTER ON LONGEVITY

TAKE-HOME POINTS

- The internet is the most popular platform fraudsters use to exploit their targets, but many still prefer to reach potential marks using traditional channels like postal mail, telemarketing and door-to-door solicitations.
- Older adults are particularly at risk for engaging with these fraudulent solicitation methods because they're more likely to be at home if a telemarketer calls or someone comes to the door.
- The best strategy to avoid fraud altogether is to resist the interaction entirely, before the fraudster has a chance to use persuasion tactics like the ones outlined in the toolkit brief "Tricks Fraudsters Use to Fool the Elderly."

The elderly are frequently solicited via unwanted phone calls from both legitimate telemarketers and fraudsters who assume seniors are lonely and looking for someone to talk to, are too polite to hang up or have assets to exploit. This brief outlines some tips for avoiding fraudulent solicitations over the phone, in the mail and at the doorstep, advice that's useful not only for the elderly but for everyone else as well. (Strategies for staying safe online are described in the toolkit brief "Avoiding Fraud 101: Cyber Safety.") Practice turning these tips into default behaviors.

AVOIDING FRAUDULENT TELEMARKETERS

DON'T PICK UP IF YOU DON'T RECOGNIZE THE NUMBER.

It's simple: If you don't recognize the name or number on your caller ID, don't answer the phone. If you don't have caller ID on your landline phone, screen calls by allowing the phone to ring until it goes to voicemail. Friends, family members, care providers and others who really want to get in touch with you will leave a voicemail and provide details on how to call them back.

HANG UP ON ROBOCALLS.

If you do answer the phone and hear a pre-recorded message--or nothing at all—just hang up. The federal Telemarketing Sales Rule prohibits pre-recorded sales messages unless you gave written permission to the organization, allowing it to contact you.[1] This means that the vast majority of robocalls are illegal. Internet-powered phone systems have made it easy and inexpensive for scammers to dial thousands of numbers simultaneously from anywhere in the world. They can even display a fake caller ID to make it look like a local number.

Because of this technology, the Federal Trade Commission has seen a significant jump in the number of consumer complaints about robocalls. Your smartest option is to ignore the call altogether or to hang up right away. Never follow pre-recorded instructions to press numbers on the keypad as this will likely lead to more unwanted calls later on.

DON'T RESPOND TO THREATS, NO MATTER HOW SCARY THEY ARE.

Fear makes people behave in ways they normally would not. That's why many scammers use threats to convince targets to comply with their requests. Some claim that they're IRS agents and say the police will arrest the targets if they don't pay immediately. These callers are imposters. Government agencies won't call people to demand payment and will never use intimidation or name-calling tactics. If you feel threatened or are told not to tell anyone about the phone call, hang up immediately. If a caller says they're with the IRS, report the call to the Treasury Inspector General for Tax Administration, either online at www.tigta.gov or by phone at (800) 366-4484. You can also report these calls to local law enforcement to inform them that scammers are fraudulently posing as police officers and threatening residents in their jurisdiction. The police may issue advisories to warn others in your community about the scam.

In general, never give any personal information to anyone who calls you on the phone, even if they claim to be a representative of your financial institution, a government agency or other service provider, and need to verify your account information. Hang up and call the company or agency directly using a phone number listed on your account statement or the organization's official website, not the number the caller provides.

ADD YOUR NUMBER TO THE NATIONAL DO NOT CALL REGISTRY.

To stop receiving annoying sales calls, add your phone number to the National Do Not Call Registry. The service is free and works for both cell phones and landlines. This will stop legitimate telemarketers from calling you. It won't stop fraudulent calls from coming in, but if you do get a sales call, you'll know automatically that it's a fraud. You can sign up online at https://donotcall.gov/ or by calling (888) 382-1222.

HOW DO YOU KNOW IT'S A SCAM?

Because legitimate telemarkers:

Can't call you before 8 a.m. or after 9 p.m.

Must immediately say the name of their business or the charity they represent and inform you it's a sales call or a call for donations.

Must disclose all information about the offer and the terms of the sale.

Can't ask you to pay with a cash-to-cash money transfer (e.g. MoneyGram or Western Union) or by telling them the PIN from a prepaid card like MoneyPack, Green Dot, or iTunes.

AVOIDING FRAUDULENT MAIL OFFERS

THROW AWAY PROMOTIONAL MAIL.

Mail that advertises discounts, free prizes or investment opportunities, or informs you that you prequalified for a loan or credit card is begging to be opened. That's because fraudsters know that people are more easily persuaded when they feel excited. To avoid getting worked up over a potentially fraudulent marketing offer, take all brochures, flyers, coupons, catalogues and marketing letters out of the mailbox and place them directly into a recycling bin—don't give temptation a chance. How do you know if it's legitimate? If the mail is addressed to "resident," "loyal customer," or anything other than your actual name, that's a clear sign that it's a piece of promotional material and should be discarded right away.

If you receive an unsolicited small prize in the mail along with a request to send money to receive a bigger prize, don't fall for it. Just keep the prize or throw it away. That little trinket is the bait that scammers send to hook you into falling for a larger scheme.

BEFORE YOU PAY A BILL, MAKE SURE IT'S REAL.

Beware of predatory billing practices. A favorite tactic among magazine subscription sales companies (and even some charities) is to send customers bogus renewal notices or fraudulent invoices. They may do this even if you already recently donated to the charity or the subscription isn't expiring anytime soon. Fraudsters also send out fake bills that closely imitate invoices from utility companies, credit card and mortgage lenders, health care and car insurers, and other services that must be paid regularly. Inspect all invoices carefully, and double check the return address on the envelope to make sure it matches the one on the bill. Keep a schedule to track when and how much was paid, and create a charitable giving plan to ensure that you only donate specific amounts to the vetted charities on your list. If you're unsure that a bill is legitimate, call the company or charity directly, using a phone number you find on their website or in the phone book, rather than calling the number listed on the letter that was mailed to you. Use sites such as GuideStar[2], CharityNavigator[3] or CharityWatch[4] to verify the legitimacy of the charity.

BEWARE OF CONTEST ANNOUNCEMENTS THAT ASK YOU TO PAY TO GET YOUR WINNINGS.

It's best to completely avoid participating in sweepstakes, lotteries and contest offers, and if you're ever informed that you won, don't fall for a request to pay the organization a deposit, insurance, or processing or service fees to receive the winnings. You'll never actually get the money, and you may be asked to fork over more. What's more, your name and contact information may be added to "sucker" or "mooch" lists that are sold to other fraudsters, causing you to be targeted repeatedly. Also, never respond to offers to repair bad credit, take out a loan or work from home. These operations are largely illegal and can't actually help you erase bad credit or make any money.

LEARN TO SPOT A COUNTERFIET CHECK.

Scammers send fake checks in the mail to get your attention and make you feel excited about the "free" money you just received. These checks may look real, but they're totally bogus. The enclosed letter will often say that the check is a pre-payment for a job or lottery winnings, or reimbursement for something you supposedly overpaid for. You'll be told to cash it, and then send a smaller amount of funds from your personal bank account to cover processing fees, taxes or some other cost. The scammer hopes that you'll cash the counterfeit check and send them money before you realize their original check was fake. You'll be stuck with the bounced check fee and lose whatever money you already sent.

REMOVE YOUR ADDRESS FROM MARKETING LISTS.

Opt out of credit card solicitation marketing lists by calling (888) 567-8688 or visiting www.optoutprescreen.com. Call your bank, insurance company and credit card issuer to ask to opt out of their marketing programs as well. You can also remove your name and address from mailing lists at http://www.dmachoice.org.

> Fraudsters know that people are more easily persuaded when they feel excited. If it sounds too good to be true, it definately is.

AVOIDING FRAUDSTERS AT YOUR DOOR

It's hard to say "no" to someone who's standing right in front of you, especially if that person is a child or claims to be collecting donations for charity. That's why door-to-door solicitations are still commonly used by religious organizations, magazine salespeople, charities and fraudsters. Here are some tips for turning them away:

PRACTICE YOUR EXIT STRATEGY.

If the doorbell rings but you're not expecting any visitors or a package delivery, consider staying put. If you do open the door to a solicitor, be armed with a message to politely decline whatever they're offering.

It's hard to say "no" to someone who's standing right in front of you.

Say "I'm sorry, but I'm not interested," or "I don't give money to solicitors." They may talk quickly or try to make you feel guilty about turning them away (this is part of the "foot in the door" technique), but stick to your prepared message and you won't feel guilty later when you find out you were duped.

DON'T TRUST A MAN IN A UNIFORM.

Just because someone looks the part doesn't mean they actually play the part. Fraudsters are excellent imposters: They may dress like city inspectors, utility workers, savvy businesspeople or even "at risk" youth to gain your trust and empathy. Never let strangers into your home or backyard. Ask to see their credentials, but know that badges and business cards are easily faked.

GET A SECOND AND THIRD OPINION ON ANY HOME REPAIR OFFER.

Fraudulent contractors find their marks by going door to door throughout a neighborhood. These scammers will insist there's a problem with your roof, drainage system or yard that they can fix at an unbeatable price, and they might even say they have materials left over from a similar job they did for your neighbor down the street. Beware of solicitors who use urgency and other high-pressure sales tactics to get you to make a decision on the spot—they just want to take your money and run. Tell them you need a second opinion before committing to any repairs. If you're concerned there's an actual problem with your property, get at least three written bids that include cost estimates on the materials and the anticipated completion date.

ACTION STEPS

1. Don't answer the phone if you don't recognize the caller.
2. Throw away promotional mail.
3. Don't "confirm" or "verify" your personal information with callers.
4. Don't send or wire money to people you don't know.
5. Don't agree to any offers where you need to pay a fee in advance or cash a large check.
6. Don't purchase, donate to or sign anything from someone who solicits you at your door.

CITATIONS

1. Telemarketing Sales Rule 16 CFR 310, Federal Trade Commission (2015). https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/telemarketing-sales-rule
2. www.guidestar.org/
3. http://www.charitynavigator.org/
4. http://www.charitywatch.org/home

The mission of the Stanford Center on Longevity is to redesign long life. The Center studies the nature and development of the human life span, looking for innovative ways to use science and technology to solve the problems of people over 50 in order to improve the well-being of people of all ages.

Stanford Center on Longevity | Stanford University | 365 Lasuen St | Stanford, CA 94305

STANFORD CENTER ON LONGEVITY