

EDUCATIONAL: DON'T BE A FRAUD TARGET

We spoke earlier about “Identity Theft and Credit Card Fraud” and the importance of protecting yourself. The following are more tips on how you can protect you and your family from other types of fraud. As we get older, we can become the target of con artists and schemes. We should especially be aware of fraud schemes for the following reasons:

- We are more likely to have a "nest egg," to own our own home, and/or to have excellent credit—all of which make them attractive to con artists.
- People who grew up in the 1930s, 1940s, and 1950s were generally raised to be polite and trusting. Con artists exploit these traits, knowing that it is difficult or impossible for these individuals to say "no" or just hang up the telephone.
- We are less likely to report a fraud because we don't know who to report it to, are too ashamed at having been scammed, or don't know that we have been scammed. We may not report crimes, for example, because we are concerned that relatives may think we no longer have ability to take care of our own financial affairs.
- When a victim does report the crime, they can often make poor witnesses. Con artists target older victims because they know the effects of age on memory, and they are counting on elderly victims not being able to supply enough detailed information to investigators. In addition, the victims' realization that they have been swindled may take weeks—or more likely, months—after contact with the fraudster. This extended time frame makes it even more difficult to remember details from the events.

What to Look For and How to Protect Yourself and Your Family

Health Care or Health Insurance Fraud

“Medical Equipment Fraud” involves equipment manufacturers offering "free" products to individuals. Insurers are then charged for products that were not needed and/or may not have been delivered. These products will also be offered in ex

"Rolling Lab" Schemes are when unnecessary and sometimes fake tests are given to individuals at health clubs, retirement homes, or shopping malls and billed to insurance companies or Medicare.

“Services Not Performed” is when customers or providers bill insurers for services never rendered by changing bills or submitting fake ones.

“Medicare fraud” can take the form of any of the health insurance frauds described above. Senior citizens are frequent targets of Medicare schemes, especially by medical equipment manufacturers who offer seniors free medical products in exchange for their

Medicare numbers. Because a physician has to sign a form certifying that equipment or testing is needed before Medicare pays for it, con artists fake signatures or bribe corrupt doctors to sign the forms. Once a signature is in place, the manufacturers bill Medicare for merchandise or service that was not needed or was not ordered.

Tips for Avoiding Health Care Fraud or Health Insurance Fraud:

- Never sign blank insurance claim forms.
- Never give blanket authorization to a medical provider to bill for services rendered.
- Ask your medical providers what they will charge and what you will be expected to pay out-of-pocket.
- Carefully review your insurer's explanation of the benefits statement. Call your insurer and provider if you have questions.
- Do not do business with door-to-door or telephone salespeople who tell you that services of medical equipment are free.
- Give your insurance/Medicare identification only to those who have provided you with medical services.
- Keep accurate records of all health care appointments.
- Know if your physician ordered equipment for you.

Tips for Avoiding Counterfeit Prescription Drugs:

- Be mindful of appearance. Closely examine the packaging and lot numbers of prescription drugs and be alert to any changes from one prescription to the next.
- Consult your pharmacist or physician if your prescription drug looks suspicious.
- Alert your pharmacist and physician immediately if your medication causes adverse side effects or if your condition does not improve.
- Use caution when purchasing drugs on the Internet. Do not purchase medications from unlicensed online distributors or those who sell medications without a prescription. Reputable online pharmacies will have a seal of approval called the Verified Internet Pharmacy Practice Site (VIPPS), provided by the Association of Boards of Pharmacy in the United States.
- Be aware that product promotions or cost reductions and other "special deals" may be associated with counterfeit product promotion.

Tips for Avoiding Fraudulent "Anti-Aging" Products:

- If it sounds too good to be true, it probably is. Watch out for "Secret Formulas" or "Breakthroughs."
- Don't be afraid to ask questions about the product. Find out exactly what it should and should not do for you.
- Research a product thoroughly before buying it. Call the Better Business Bureau to find out if other people have complained about the product.
- Be wary of products that claim to cure a wide variety of illnesses—particularly serious ones—that don't appear to be related.

- Be aware that testimonials and/or celebrity endorsements are often misleading.
- Be very careful of products that are marketed as having no side effects.
- Question products that are advertised as making visits to a physician unnecessary.

**Always consult your doctor before taking any dietary or nutritional supplement

Telemarketing Fraud

Telemarketing scams often involve offers of free prizes, low-cost vitamins and health care products, and inexpensive vacations. There are warning signs to these scams. If you hear these—or similar—“lines” from a telephone salesperson, just say "no thank you," and hang up the telephone:

- "You must act now, or the offer won't be good."
- "You've won a free gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.
- "You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.
- "You don't need to check out the company with anyone." The callers say you do not need to speak to anyone, including your family, lawyer, accountant, local Better Business Bureau, or consumer protection agency.
- "You don't need any written information about the company or its references."
- "You can't afford to miss this high-profit, no-risk offer."

Tips for Avoiding Telemarketing Fraud:

It's very difficult to get your money back if you've been cheated over the telephone. Before you buy anything by telephone, remember:

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware—not everything written down is true.
- Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.
- Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.

- Before you give money to a charity or make an investment, find out what percentage of the money is paid in commissions and what percentage actually goes to the charity or investment.
- Before you send money, ask yourself a simple question. "What guarantee do I really have that this solicitor will use my money in the manner we agreed upon?"
- Don't pay in advance for services. Pay services only after they are delivered.
- Be wary of companies that want to send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.
- Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.
- Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- Before you receive your next sales pitch, decide what your limits are—the kinds of financial information you will and won't give out on the telephone.
- Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor. It's never rude to wait and think about an offer.
- Never respond to an offer you don't understand thoroughly.
- Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.
- Be aware that your personal information is often brokered to telemarketers through third parties.
- If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.
- If you have information about a fraud, report it to state, local, or federal law enforcement agencies.

Internet Fraud

As web use among citizens increases, so does their chances to fall victim to Internet fraud. Internet Fraud includes non-delivery of items ordered online and credit and debit card scams.

Investment Schemes

Investment schemes may include advance fee schemes, prime bank note schemes, pyramid schemes, and Nigerian letter fraud schemes.

Reverse Mortgage Scams

The FBI and the U.S. Department of Housing and Urban Development Office of Inspector General (HUD-OIG) urge consumers, especially senior citizens, to be vigilant when seeking reverse mortgage or home equity conversion mortgage (HECM) products.

Reverse mortgage scams are engineered by unscrupulous professionals in a multitude of real estate, financial services, and related companies to steal the equity from the property of unsuspecting consumers or to use them to unwittingly aid the fraudsters in stealing equity from a flipped property.

In many of the reported scams, victims are offered free homes, investment opportunities, and foreclosure or refinance assistance. They are also used as straw buyers in property flipping scams. Consumers are frequently targeted through local churches and investment seminars, as well as television, radio, billboard, and mailer advertisements.

A legitimate HECM loan product is insured by the Federal Housing Authority. It enables eligible homeowners to access the equity in their homes by providing funds without incurring a monthly payment. Eligible borrowers must be 62 years or older who occupy their property as their primary residence and who own their property or have a small mortgage balance.

Tips for Avoiding Reverse Mortgage Scams:

- Do not respond to unsolicited advertisements.
- Be suspicious of anyone claiming that you can own a home with no down payment.
- Do not sign anything that you do not fully understand.
- Do not accept payment from individuals for a home you did not purchase.
- Seek out your own reverse mortgage counselor.

If you are a victim of this type of fraud and want to file a complaint, you can submit information through the FBI's electronic tip line or through your local FBI office. You may also file a complaint with HUD-OIG at www.hud.gov/complaints/fraud_waste.cfm or by calling HUD's hotline at 1-800-347-3735.

The Latest Phone Scam Targets Your Bank Account

Imagine getting hundreds or thousands of calls on your home, business, or cell phone, tying up the lines. And when you answer, you hear anything from dead air to recorded messages, advertisements, or even phone sex menus.

It's annoying, no doubt. But it could be more than that—it could be a sign that you're being victimized by the latest scam making the rounds. This "telephone denial-of-service attack" could be the precursor to a crime targeting your bank accounts.

Denial-of-service attacks, by themselves, are nothing new—computer hackers use them to take down websites by flooding them with large amounts of traffic.

In a recent twist, criminals have transferred this activity to telephones, using automated dialing programs and multiple accounts to overwhelm the phone lines of unsuspecting citizens.

Why are they doing it? Turns out the calls are simply a diversionary tactic: while the lines are tied up, the criminals—masquerading as the victims themselves—are raiding the victims' bank accounts and online trading or other money management accounts.

Here, in a nutshell, is how the whole thing works:

- Weeks or months before the phone calls start, a criminal uses tactics to obtain personal information—like account numbers and passwords. Perhaps you responded to a bogus e-mail, inadvertently gave out sensitive information during a phone call, or put too much personal information on social networking sites that are trolled by criminals.
- Using technology, the criminal ties up the victim's various phone lines.
- Then, the criminal either contacts the financial institution pretending to be the victim...or pilfers the victim's online bank accounts using fraudulent transactions. Normally, the institution calls to verify the transactions, but of course they can't get through to the victim over the phone.
- If the transactions aren't made, the criminals sometimes re-contact the financial institution as the victim and ask for it to be done. Or they add their own phone number to victims' accounts and just wait for the bank to call.
- By the time the victim or the financial institution realizes what happens, it's too late.

Law enforcement and industry response.

To help fight these schemes, the FBI has teamed up with the Communication Fraud Control Association—comprised of security professionals from communication providers—to analyze the patterns and trends of telephone denial-of-service attacks, educate the public, and identify the perpetrators and bring them to justice.

Ultimately, though, it's individual consumers and small- and medium-sized businesses on the front line of this battle. So take precautions: never give out personal information to an unsolicited phone caller or via e-mail; change online banking and automated telephone system passwords frequently; check your account balances often; and protect your computers with the latest virus protection and security software..

Another resource to assist you is the Adult Protective Services (APS) unit. This unit oversees investigations into reports of possible maltreatment of vulnerable adults. It also helps the vulnerable adult and caregiver find and receive services that are acceptable to the adult to help keep them as safe and healthy as possible. APS unit contact information:

APS
Sequoyah Memorial Office Building
2400 Lincoln Blvd.
Oklahoma City, OK 73105
Phone: (405) 521-3660 or (800) 522-3511

If you think you may have been targeted by any of the above crimes, act immediately by contact the company it affects (i.e. insurance company, financial institution, your telephone provider, etc) Also, file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov.

Joyce Gibson
Oklahoma State Council 2010-2011
2nd Vice President/Educational Chairman

Resources:

- Federal Bureau of Investigation
- Adult Protective Services in Oklahoma City
- USA.gov Resources for Seniors
- Resources from the United States Senate Special Committee on Aging