Scams against Seniors

Presented in collaboration with Crime Prevention Specialist Officer Steve Watson

Federal Grant Scams

Consumers receive a phone call saying they have been selected by a government agency to receive a free grant of which does not have to be repaid. The caller then asks for the consumer's bank account information so the money can be transferred into the account.

- Don't give any account information to anyone you do not know
- Don't pay for "free" government grants
- There is no agency called "Federal Grants Administration" . The only official access point for all federal grant-making agencies is www.grants.gov.

Telemarketing Scams

The phone is an easy way for telemarketers to sell their goods. If you are tempted by the offer, you had better get the facts before a potential fraud gets you. There are many unscrupulous companies involved in telemarketing fraud. Fraudulent telemarketers use phony prizes, cheap products and high-pressure tactics to defraud consumers. Seniors are 3 times as likely to become victims of telemarketing fraud.

- Don't be pressured to make an immediate decision. TAKE YOUR TIME TO THINK ABOUT IT!!!
- **Don't give your credit card, checking account or Social Security number to unknown callers.**
- Don't pay for something because you'll get a "free gift."
- Take control of the calls you receive. If you want to reduce the number of telemarketing calls you receive, place your telephone number on the National Do Not Call Registry. To register online, visit www.donotcall.gov. To register by phone, call 1-888-382-1222 (TTY: 1-866-290-4236) from the phone number you wish to register.
- Check out the charity before you give any money. Ask how much of your donation actually goes to the charity. Ask that written information be sent to you so you can make an informed decision.
- Don't invest your money with an unknown caller who insists you make up your mind immediately
- Scam operators , often based in Canada, are using the telephone and direct mail to entice U.S. consumers to buy chances in high-stakes foreign lotteries from as far away as Australia and Europe. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail. Consumers are lured by prospects of instant wealth. Participating in foreign lottery, through the mail or telephone, violates federal law because it is illegal to transfer funds across borders.
- There are no secret systems for winning foreign lotteries. Your chances of winning more than the cost of your tickets are slim to none. If you purchase one foreign lottery ticket, expect many more bogus offers for lottery or investment opportunities. You will be placed on "sucker lists" that fraudulent telemarketers buy and sell.

Phone Scams

This scam often targets seniors by claiming family members are in legal trouble or hurt in an accident.

- No law enforcement officer will call to say they can get a family member out of jail for a fee or solicit bail money
- Never send money when asked to use Wal Mart or Western union exclusively
- Try to make contact with the family member that is supposed to be in trouble
- Ask for the name of the facility that is holding your family member and attempt to make contact
- Always ask to speak to the family member that they say is being held in jail
- Always ask the person claiming to be your grandchild a question only they would know
- Never respond with the grandchild's name until they identify themselves by their own name

Identity Theft

- Never purchase products online from unsecure sites. Verify "https" "SSL sites"
- Shred all bills and mail that contain identifying information.
- Never give out personal information over the phone unless you initiate the call.
- Never leave outgoing mail in the mailbox for extended periods of time. Drop it off at the Post Office.

Sweepstakes and Fake Checks

Always be very suspicious of offers that will allow you to get paid to work at home or receive an "advance" on a sweepstakes you have supposedly won. Under the Virginia Prizes and Gifts Act, if you are told you have won a prize or gift, you do not have to submit to a sales pitch or pay any money in order to receive your prize or gift. You must be given your prize within ten days, without any obligation. Your prize notification is also required to contain information which reveals the retail value of each prize, the odds of winning each prize, the exact number of prizes to be awarded and what conditions must be met to receive the prize. Shipping charges for the prize cannot exceed the cost of postage or delivery service, and the handling charges cannot exceed the lesser of the cost of handling or $5.

- Do not pay to collect sweepstakes winnings. Legitimate sweepstakes do not require you to pay "insurance," "taxes" or "shipping and handling charges" to collect your prize.
- Hold on to your money. Do not be pressured to wire money or send it by overnight delivery. Con artists recommend these services so they can get your money before you realize you have been cheated.
- Look-alikes are not the real thing. Disreputable companies sometimes use a variation of an official or nationally recognized name to try to confuse you. Insurance companies, including Lloyd's, do not insure delivery of sweepstakes winnings.
- Phone numbers can deceive. New technology can make incoming calls look as if they are coming from Washington, DC, or your own community.

The most visible form of this fraud is the Nigerian Letter. Originally, the schemers contacted mainly heads of companies and church officials, often by fax or postal mail. However, the use of e-mail spam and instant messaging for the initial contacts has led to many private citizens also being targeted, as the cost to the scammers to make contact is much lower. A typical letter comes from a person needing to transfer large sums of money out of the country or from a lottery company. If you receive a letter from Nigeria, asking for personal or banking information, do not reply! Send the letter to U.S. Secret Service or the FBI.

Medicare Scams

Seniors are frequent targets of Medicare fraud, especially for medical equipment such as Diabetic supplies or Mobility Equipment. They offer free medical supplies and products in exchange for your Medicare numbers.

- Most Medicare payment errors are simple mistakes and are not the result of physicians, providers, or suppliers trying to take advantage of the Medicare system. If you have a question or concern regarding a Medicare claim submitted on your behalf, you should discuss it directly with your provider or supplier that provided the service.
- Don't give your Medicare Health Insurance Claim Number (on Medicare card) except to your physician.
- Don't allow anyone, except medical professionals, to review your medical records or recommend services.
- Do be careful in accepting Medicare services which are represented as being " free" such as free testing or screening in exchange for your Medicare card number.
- Never sign blank insurance forms.
- Never give blanket authorization to a medical provider to bill for services rendered.
- Never give out your Medicare number over the phone or the internet if you did not initiate the communications.
- Review all medical bills carefully for unauthorized billing for services. Know if your physician ordered equipment for you.

Phishing Scams

"Phishing" (also called "spoofing") occurs when thieves send an e-mail which appears to have been sent from the domain of a legitimate retailer, bank, credit card or insurance agency. Fraudsters have spoofed customers of Citibank, BestBuy, Earthlink, eBay, PayPal and even the Federal Deposit Insurance Corporation (FDIC). The email asks the recipient to update their account information for banks, credit cards, online payment services or popular shopping sites. Frequently, the email claims the recipient's account information has expired or has been lost and the account holder needs to immediately resend it to the company.

- Be extremely skeptical of email received from someone you don't know. Never respond to any request for personal information that comes to you via email.
- Keep separate passwords for each online account.
- Never click on a link embedded within any potentially suspicious email.
- Call your financial institutions to verify account status before divulging any information.

Fraudulent Charities

The ease and convenience of shopping online has led an increasing number of consumers to purchase goods and services on the Internet. In the process, customers transmit personal information such as their Social Security Numbers, and credit card numbers through cyberspace. While some of these web sites are safe and serve their purpose well, others either do not have the proper security measures or present a fraudulent front with the sole purpose of gaining personal information.

- Benevolent organizations: "Police", "Fire", "Veteran Organizations", Children's Funds, International Religious Outreach and Political Organizations
- Do not provide your credit card number unless the site is secure and reputable. Look for indicators that the site is secure, e.g., a "lock" icon on the browser's status bar, or a URL that begins with "https:" (the "s" stands for "secure) . Look for symbols such as the Better Business Bureau's Online Reliability and Privacy Seals and the TRUSTe privacy seal.
- Check the website's privacy policy so you can be assured you have full control over the uses of your personal information.
- Pay by charge or credit card. If you pay by credit or charge card online, your transaction will be protected by the federal Fair Credit Billing Act. This statute gives you the right to dispute charges under particular circumstances, including unauthorized charges, charges that list the wrong amount or charges for goods which were not delivered. NEVER GIVE CASH!
- Research the organization before you donate. Ask for written information before donating.
- Never believe that the charity's budget is based on your immediate donation. Never donate to an organization that only accepts money by phone.

Phone Bill Scams

If you see Additional user fees, activation fees, member fees, web hosting, voicemail, or ringtones on your phone bill, you could be a victim of Cramming. Check your phone bill for fees you did not sign up for or have recently started to appear on your monthly bill.

- Cramming happens when a company adds a charge to your phone bill for a service you didn't order, agree to, or use. Cramming charges can be small, say $2 or $3, and easy to overlook. But even when the phony charges aren't small, they may sound like fees you do owe. That makes them tough to pick out, especially if your phone bill varies month to month.
- Ask your phone company about it..If the charge isn't from your phone company, the name of the company charging you should be printed nearby. Your phone company should be able to tell you more about the charge.
- Dispute it - Your statement should tell you how to dispute errors on your bill.

- Follow-up with an email or letter sent by certified mail, and ask for a return receipt. It's your proof that the company received your letter. Keep a copy of your bill and any other documentation for your files.
- File a complaint if it sounds too good to be true. When you suspect a con or a fraud, please call the Police.

Home Improvement Scams

Don't allow anyone to come to your door and suggest you need some type of home repair immediately (driveway paving, roof repair, tree trimming, etc). If you are asked to make a decision quickly, decline! Always check references and credentials before starting a business relationship.

Protect yourself against scams and frauds

1. If it sounds too good to be true – it probably is!
2. When you suspect a con or a fraud, call your local police immediately.
3. Ask for ID from salespeople/solicitors.
4. If you have a problem with a business, call the Virginia Attorney General's Office or the Virginia Department of Agriculture and Consumer Services.
5. Call your financial institutions immediately if your checks/credit cards have been lost or stolen.
6. Call the Fraud Unit of all major credit reporting agencies to report a fraud alert.
7. Remove your name from the telemarketer list by signing up at www.donotcall.gov or call 1-888-382-1222.
8. Stop direct mail and telemarketers by writing to:
   Direct Marketing Association
   PO Box 9008
   Farmingdale, NY 11735
9. Review helpful information on http://www.usa.gov/topics/consumer.shtml
   - Know your rights and responsibilities before you make a purchase, and learn how to protect your rights after you buy
   - Order a copy of the current Consumer Action Handbook.
   - Protect yourself against the latest scams to get your money.
   - How to file a comsumer complaint. Get a sample complaint letter template to contact the sellers, manufacturers, or consumer organizations.
10. Knowledge is a powerful tool. Learn to recognize the signs of scams so as not to fall victim to them.

Home Instead
SENIOR CARE
To us, it's personal.
www.homeinstead.com
434-979-4663