Copies of UARA Newsletter Articles on Scams and Fraud
Published in January 2013 and April 2013 Issues (UA Retirees Association)
uara.arizona.edu/newsletters/scams-fraud.pdf

Part 1 (in UARA January 2013 Newsletter)

Scams, Fraud, and Identification Theft: Part 1

By Roger Caldwell, Webmaster

Part 1 of this article covers the most common types of scams and fraud, defines the key terms, lists the primary agencies involved, and summarizes steps for your protection. Part 2 will be in the April newsletter and will cover specific examples and defensive solutions to protect yourself.

The UA

RA Fall Educational Seminar (October 16) on Fraud and Identity Theft was given by Sheriff's Department Detective Brian Greeno. He provided a very informative (and humorous) session and stayed after the session to continue answering questions. This article summarizes some of Detective Greeno's comments but also expands the types of examples and lists additional sources of information.

There are many forms of scams and fraud. People involved can be contacted through multiple methods. The specific issues may change, but the overall themes have been around awhile. Learn how to recognize possible scams and fraud, how to check if legitimate, and where to get additional information. There is not a shortage of information on types and solutions of fraud and scams. Primary sources are the various Better Business Bureaus, State Attorney's General Offices, Federal Trade Commission, Federal Bureau of Investigation, and the U.S. Government Accountability Office.

Definitions

A *SCAM* is a fraudulent scheme to make a quick profit. Related terms include: con game, hustle, swindle, and bamboozle.

FRAUD is intentional deception or dishonesty for personal gain or damage to someone. It includes false representation of a fact by a seller or advertiser of merchandise or job opportunities.

DECEPTIVE ADVERTISING is where a statement is made in large print or in an easily understandable voice, but then has a disclaimer in fine print or a rapidly speaking voice that indicates the exceptions, additional requirements, or language that is not easy to understand (note these disclaimers are required by the FTC).

IDENTIY THEFT is theft of someone's personal information (examples include social security number, credit cards, bank account number, or birthdate).

Federal Bureau of Investigation Common Frauds and Scams

1. Telemarketing fraud.
2. Nigerian Letter and other advance fee schemes.
3. Funeral and cemetery fraud.
4. Investment schemes or auction frauds.
5. Reverse mortgage schemes.
6. Health care or health insurance fraud.
7. Counterfeit prescription drugs or fraudulent "anti-aging" products.
8. Non-delivery of merchandise.
9. Ponzi or pyramid schemes.
10. Identity theft.

Better Business Bureau (National): Top 10 Scams (2011)

1. Job Scam (you passed interview, now fill out a credit form).
2. Lottery (via email, click and the spammer gets your personal information).
3. Upgrade your flash player (click this and it downloads a virus).
4. Home improvement (person does shoddy work but takes the money and runs).
5. Check cashing (wrote the check for too much, wire me the difference).
6. Phishing (provide bank account information).
7. Identity theft (hotel [fake] "front desk" indicates problem with credit card).
8. Financial (keep overdue mortgage by sending us money).
9. Sales (auction bid on iPad, but you pay just for the bidding process).
10. BBB Phishing (BBB complaint to business, downloads malware to get bank info).

Ways You are Exposed

Scams and fraudulent activities can be conducted through the mail, phone, internet (web or email), credit cards, knocking on your door, and other vehicles such as submitting your taxes.

Scams are especially prevalent by telephone and email: a) you are asked to wire a large amount of money to someone you know to get them out of jail (but it is not the person you think asking the question); b) you are told you can receive a large amount of money (usually from Africa) if you just give them your bank account number; and c) you are asked by your bank or phone company (or others) to update your account information (submitting your account name and password). Note: Legitimate companies and organizations do not ask for your password via email.

Financial Exploitation

This can be by a person who is known to the victim, such as a family member, caregiver, or someone acting with a power of attorney. Or, it can be a stranger such as an unscrupulous salesman or a con artist.

Persons working with elderly may notice some warning signals, such as withdrawals from financial

accounts that seem inconsistent with normal behavior, change in beneficiaries, or changes in legal documents.

Red Flags of Identity Theft

1. Mistakes on your financial statements or medical benefits.
2. Regular bills/statements don't arrive on time.
3. Call from debt collectors or collection notices.
4. A notice from IRS that someone used your social security number.

Having your identity stolen is a difficult recovery path – prevention is easier! If it is stolen, there are a series of steps you must go through. These include notifying the credit reporting agencies (quickly), submit an identity theft report with the FTC by calling them at 1-877-id-theft (1-877-438-4338).

Summary of Key Steps for Your Protection

1. Do not put bank statements in the trash. It is better to read them electronically and to shred any paper copies (cross-cut shredders are best).
2. Minimize number of credit cards.
3. Check bank and credit card accounts often for irregular activity. Notify authorities of irregularities in financial statements.
4. Review free copies of your credit reports (one from each report provider; 3 total per year).
5. Put valuable papers in a safe place.
6. Protect computer passwords (consider a password manager).
7. Use encrypted router (almost all are) for connecting to internet.
8. Do not give private information to someone who calls you on the phone. Do not consider any phone offer to send money to someone.
9. Don't keep personal information in the car (or leave your purse on the seat).
10. Remember, if something sounds too good to be true, it probably is not true.

In Part 2, to be published in the April 2013 newsletter, we will cover examples and how to defend yourself against scams and fraud. Thanks to Detective Brian Greeno of the Financial Crimes Division, Pima County Sheriff's Department, Nick LaFleur of the Southern Arizona Better Business Bureau, and Kenney Hegland, retired UA Professor of Law for reviewing a draft of this article. Additional links to fraud and scam information are on the UARA website, and a copy of both parts of this newsletter article is available as a single pdf file at uara.arizona.edu/newsletters/scams-fraud.pdf

Part 2 (in UARA April 2013 Newsletter)

Scams, Fraud, and Identification Theft: Part 2

By Roger Caldwell, Webmaster

The UARA Fall 2012 Educational Seminar (October 16) on Fraud and Identity Theft was given by Sheriff's Department Detective Brian Greeno. He provided a very informative (and humorous) session and stayed after the session to continue answering questions. This article summarizes some of Detective Greeno comments but also expands the types of examples and lists additional sources of information. Part 1 covered primary agencies involved, definitions, types of common complaints, and how you are exposed to scams and fraud. Part 2 covers examples and defensive solutions to protect yourself.

Email "phishing" Message: phishing email is sent to many people in hopes some will bite. You get a message like *"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."* Often this type of message gives you a clue to its real meaning, but you need to how to find the clue. If you roll your computer mouse over the link in the message (don't click, just move the mouse over it), you will see the real address – which can be different than the one shown on the screen. If the link is different than the one indicated on the screen, do not use that site. If the link has a two digit final entry that tells which country it came from; you can see the list of country codes at theodora.com/country_digraphs.html (note underscore after "country"). Another clue is to see who else is receiving the message. Often there is a long string of names and you will not recognize most or all of them. This is a clear signal it is junk mail or worse.

Insurance Fraud: You are urged to change policies that seem to be perfectly good, overstating benefits or selling unsuitable policies to someone in your situation. Do your homework and ask questions, do not sign up immediately.

Disaster Relief: When natural disasters or other crises occur, pop-up charities spring up quickly. It is better to use established charities. For more information to http://ftc.gov/charityfraud

Grandchild Calling: : Someone calls claiming to be your grandchild or calls on their behalf and asks you to wire money to them . Today people can find out a lot about other people through Facebook and other social media, making it relatively easy to appear to be the real grandchild.

Advertising – You Decide if it is Deceptive or Not: You can get inexpensive internet access for multiple years (but the fine print notes you must also meet other requirements such as have phone service). A variety of services and health supplements of all types are common examples.

Medicare Scams and Fraud: Medicare fraud is billing for services or supplies that are not provided. There is a range of ways this is done, including:

1. *Phantom Billing:* a provider bills Medicare for procedures that were not performed or were unnecessary. Or billing for home health care for those than can still drive.
2. P*harmaceutical pricing*: a manufacturer pays a prescription benefit manager a kickback to list their drug.
3. *Durable medical equipment*: billings for things like wheelchairs that do not meet Medicare coverage guidelines, or improper marketing or sales door to door.
4. *Nursing homes:* bill Medicare for multiple payers (Medicare and private insurance companies) allows complex billing opportunities and "vulnerabilities" in the system.
5. *Medicare plans:* a company uses false information to mislead you into joining a Medicare plan.

Arm Yourself by Being Defensive: Keep alert, if something seems too good to be true, it probably is not true. Before buying something you need to know where an offer is coming from and who you are dealing with. Don't send money to someone you don't know. Don't respond to messages asking for personal or financial information. Read financial statements or bills (online or paper) regularly to see if there are any unexpected charges. Keep a good security program on your computer and do not respond to questionable phone calls or email.

Sign up for the FTC's National Do Not Call Registry for your phone (including cell at https://donotcall.gov) or call 888-382-1222 from the phone you want to register. Cell phones should be less of a problem because federal law prohibits automatic dialers from calling cell phones. Registration will not expire once you have entered your phone number.
Minimize your credit cards (e.g., retain one major credit card for each spouse and get rid of the rest). Monitor your financial statements and take advantage of free annual credit checks. The three primary credit agencies must each give you one **free statement** per year**,** required by the Fair and Accurate Credit Transactions Act (FACT Act) of 2003. So you can get three time periods by requesting these statements at different times.

The three organizations are: Experian, TransUnion, and Equifax. There is a single website, sponsored by all three organizations, to get any of these reports. The website is also informative about what is in the reports, a description of the FACT Act, and a Frequently Asked Questions section that gives advice on how to flag your record if you have been subject to fraud. Go to annualcreditreport.com.

Take care with your credit cards as they have a lot of information about you on the magnetic strip, including your name and bank account number. An unscrupulous organization could take your credit card into another room, scan it, and keep the information.

Mail theft is becoming more common. The thief quickly checks the mail for financial information and can make fake credit cards or bank withdrawal identification in minutes after getting your mail. The solution here is to use a post office box or a well-made locking mailbox (some locking mailboxes and be easily broken into).

What To Do If You Think You Are a Victim

You can file a complaint with these organizations:

1. Southern Arizona Better Business Bureau (tucson.bbb.org).
2. Arizona Attorney General (azag.gov/consumer).
3. Federal Trade Commission (ftc.gov/bcp/index.shtml), or many consumer-oriented organizations. Name identity theft – (idtheft.gov).

Thanks to Detective Brian Greeno of the Financial Crimes Division, Pima County Sheriff's Department, Nick LaFleur of the Southern Arizona Better Business Bureau, and Kenney Hegland, retired UA Professor of Law for reviewing a draft of this article. Additional links to fraud and scam information are on the UARA website, and a copy of both parts of this newsletter article is available as a single pdf file at uara.arizona.edu/newsletters/scams-fraud.pdf

rlc