# Scams & Con Games

Listed below are some of the most common scams and con games. Many of these cons have been around for centuries yet still managed to find new victims.

Please pass this information on to family members that may not be aware of these types of scams. Con artist scams occur throughout all neighborhoods. Just because someone appears to be legitimate and you feel a need to save or make money, don't be fooled.

Report suspicious activity to your local police. If it sounds to good to be true, it probably is!

## ATTORNEY GENERAL - BE WARY OF ID THEFT

Texas Attorney General Greg Abbot is warning Texans to watch for signs of fraud, as the Federal Trade Commission has identified Texas as second in the nation for identity theft complaints.

Nearly 32,000 Texans were identity theft victims in 2008, according to the FTC. While the average victim loses hundreds of dollars and spends several hours cleaning up the damage, the worst cases can cost thousands of dollars and take years to fully repair.

The Office of the Attorney General has warned that there are several ways thieves can find victims, from retrieving bills and other documents from the trash to using fake emails to get victims to provide personal information. Other methods include theft of credit cards and identification, using viruses to gain financial and personal information and phony job offers requiring the applicant to divulge sensitive information. A full list of methods and ways to protect from identity theft is available on the AG's Web site.

The AG also recommends that people regularly review financial statements to watch for unusual activity and that they review credit ratings at least annually. If you believe your identity has been stolen, the AG recommends to first request a credit report "Fraud Alert", which requires special steps before any new accounts are created and changes are made to existing credit accounts.



## Brazos Valley Schools Credit Union Phishing Scam

Brazos Valley residents are again the target of a phishing scam intended to obtain credit card and other personal information by telephone, email and text messages. The scammer typically tells the intended victim that their credit card, debit card, or ATM card has been deactivated because of suspected fraudulent use. If the initial contact has been made by phone, the scammer then asks the victim to press 1 for more information, followed by prompts to enter the credit/debit card number. The scammer often identifies him/herself as "Brazos Valley Schools Credit Union". Please remember that credit card issuers will never contact you by phone, email or text messages and ask you for your credit card number or personal identity information.

For more information please see the Brazos Valley Schools Credit Union website at http://bvscu.org/.

Credit card scam targets Brazos Valley residents - Bryan-College Station Eagle (3.10.2009)

# Scams & Con Games

## BANK EXAMINER SCAM

A male or female purporting to be a law enforcement officer complete with badge to get your attention, will either phone or approach you and explain that they need your assistance to catch a corrupt bank employee. The con artist (fake cop) will inform you that the local bank teller at your bank is stealing your money every time you make a transaction.

The con artist will further tell you that they need you to make a withdrawal and they will be able to prove to you that the suspect teller actually withdrew more cash than you requested and kept the difference. The con artist will inform you to keep this matter strictly confidential. The con artist may even meet you in a public place, such as a library, in order to go over the details of their investigation.

You will feel a need to cooperate as this is your money and you don't want to be deceived by the corrupt bank teller. You meet the fake cop at the bank and he may even arrange for a cab ride for you. The con artist will direct you to make a substantial withdrawal and ask you to turn it over to them in order to document the bills and complete the investigation. The only problem is soon after you turn over your cash to the fake cop/con artist, the con and the cash will vanish in the parking lot.

Real Cops don't need you to withdraw money to investigate these types of matters. Real Cops will either use loss prevention personnel at the bank, other bank employees, plain-clothes police officers, or other sources.

## DOOR-TO-DOOR SALES

Often, con artists will try to get you to subscribe to a magazine or offer a cure for a medical condition. A con may also offer a free inspection of your home for problems with your furnace, hot water tank, appliance, or garage door. Whatever the con has to offer, simply say no and report them to your local police.

More than likely they need to have a solicitor or business license of some type from your local city hall in order to conduct such door-to-door business. The con may even have an I.D. that appears to have been issued by your local government office. Check it carefully.

Don't get tangled in the net by these con artists that may offer to perform electrical, plumbing, and related work. Anybody can have stationery printed in no time that looks to be legitimate.

You worked too hard for your money, don't give it away. Get a referral from a neighbor for work that needs to be performed and consult the yellow pages.

## DRIVEWAY AND ROOF REPAIR SCAMS

A male will approach you and offer to fix that roof leak you have or seal coat your driveway. The price will be reasonable and they offer to work cheap in exchange for cash. The con artist may

even have a letterhead that looks to be legitimate. Due to the low cost you may agree to have the work performed immediately.

The con artist will simply use a silver color paint to brush around the flashing making it look like he is hard at work on your roof. The con may offer to seal coat the driveway in a similar fashion and simply apply some old motor oil to the dull surface making it look good as new, until the first rain.

In either case the con really wants the cash you have hidden within your home in addition to the fee he charged for the supposed "work". Here's how he'll get it.

The con will ask to use your bathroom or telephone. His partner may engage you in a conversation to distract your attention while the con roots through your dresser drawers and jewelry boxes. They know where to look and are familiar with all the "secret" hiding places most homeowners' use. They can pick you clean in just minutes.

## FLAT TIRE/GOOD SAMARITAN ALERT

After conducting business at your local bank, check your tires and see if they appear to be low on tire pressure or flat. Cons have been known to either puncture or slash a tire on your car knowing the tire will soon be flat. The con will follow you from the bank parking lot and offer to help with the flat tire. The con usually targets the elderly knowing they will normally accept the offer of assistance. The cons may travel as a husband and wife and appear friendly and non-threatening. As soon as one of the cons begins working on the flat tire the other will be working on cleaning out your purse.

## FOOL'S GOLD

A male will approach you and explain that he recently separated with his girlfriend or has recently stolen the 14K ladies ring that he now has in his hand and that he needs fast cash. The male may go on to tell you that he was just laid off from his job. The con may even tell you how the money will pay for food and a fill up for his car, as of course he just ran out of gas.

The story and the ring look pretty good. You make an offer and feel real good about the great deal you just negotiated. The only problem is that the ring is of little if any value and the 14K stamp is MO-JO.

## LOST PUPPY TRICK

Also be on the alert during summer months when you're out in your yard for a con artist family that pretends to be looking for their lost puppy. These same con artist are the same people doing the roof and driveway jobs, but they just ran out of silver paint and old motor oil.

While you are helping them find the lost puppy, some of the family members will be inside your home looking for cash and other items of value. Don't be taken by the family traveling with children, as they too are part of the diversion. A popular variation of the lost puppy is to have the child ring the doorbell and beg to use the washroom. The child will appear to be in obvious

distress. You let the kid in to use the bathroom while mom or dad engages you in conversation. While you are distracted the child goes through your things, pocketing cash and jewelry.

Keep your doors locked at all times, even if you are just out in the back yard for a few minutes, that's all the time they need to seek and find.

If you need your roof repaired or driveway seal coated check with a neighbor and get a referral, check your local yellow pages, or find a trustworthy handy man. Also check with your local city or township office and see if they have a list of competent sources to perform the work in question.

When in doubt, investigate first, before it's too late. Notify the local police if you suspect some type of scam going down or if you see what you believe to be a scam going on at the home of an elderly neighbor.

## LOTTERY TICKET SCAM

A con will seek you out and offer to share with you the windfall from a winning lottery ticket. The con will explain how he/she is unable to claim the winning ticket because he/she is either going through a divorce and can't claim the money or is on a work related injury and is receiving benefits that will be reduced.

The con may even have another third party involved to verify the validity of the ticket. You will in turn feel the need for greed and give the con artist a sum of cash in exchange for the winning lottery ticket.

I don't think I have to tell you the ending to this story if you have been paying attention.

## METER READERS - CENSUS WORKERS - POLICE OFFICERS

Be on the look out (BOLO) for strangers appearing at your door purporting to be utility workers from the telephone, electric, or gas company. These con artists for the most part target the elderly. The con artist simply wants to gain entry and find the cash kept in the home.

Keep your distance and verify their credentials by calling their office. These innocent property crimes can go bad and turn into violent crimes. Unfortunately there are con artist that go one step further and identify themselves as police officers in order to gain entry into your home. Don't hesitate to question ones identity.

Call the police and check the validity of these officers if in doubt, they will be glad to assist you and will understand your concern. Dial 911 for an emergency. Better to be Safe than to be Sorry.

It may be time to purchase an inexpensive intercom system that is easily installed. This way you don't have to have any face-to-face contact with a con artist and you can summon the police before its too late.

# Scams & Con Games

## PIGEON DROP

A female, male or any combination of will approach you and either show you a large amount of cash or tell you about the large sum of money that they just found. The con artist may explain that whoever lost the cash must have obtained it unlawfully. He will offer to share the wealth with you, but first you will need to put up some cash in order to show your good faith. The con artist will encourage you to make a withdrawal at your local bank. In most cases the con artist does not have any cash to show you on the spot, but has had a third party approach the scam and offer to bring you back your share as a responsible employer is holding on to the loot. If the con artist has shown you the found cash and offered to share with you on the spot, after you hand over your good faith money, then all you will find is a few small bills wrapped around a lot of nothing.

The bottom line is not to fall for any story about any found cash and sharing in the wealth.

## TV SCAMS

You will be approached by a male con artist, who shows you a brand new portable TV. He offers to sell you one still in the box. The con artist will tell you that he has a few available as they fell off the truck, if you know what I mean. The price will be good and the TV is just the thing you need.

The con will sell you a brand new one in the box. You can't wait until you get home with your new TV. Luckily for you the con only sold you one box of bricks in a TV box.

Another TV Scam is targeted for only the high roller/professional. The con will find your company listed in a local phone book and call your office. The con will explain that he just happened to find himself in the neighborhood and has a tractor-trailer full of TVs for sale. The con explains that he is just a block or two away at a local restaurant and is willing to meet with you if you keep the matter confidential, as the TVs have just been stolen from a retail store at a local shopping center.

You meet the con at the restaurant and discuss price for the entire load of TVs. The con wants you to get the cash together immediately and rent a truck suitable to hold the load of TVs, as they currently are stored in a trailer waiting at a loading dock.

The con will have you drive him to the shopping center in order to view the trailer load of TVs. The con will simply pick out a trailer backed into a retail store of the mall and explain how the driver is in on the deal/theft.

You hurry up and come back with the cash and the truck. You give the con a ride back to the loading dock, as he needs to confirm everything with his partner at the dock. The con artist jumps onto dock or enters a small door near loading dock to show you he is legit.

After a few hours you investigate and find the real driver of the tractor-trailer and discover the con is long gone. The con made his way from the dock area to the mall and is still laughing.

# Scams & Con Games

## VIRUS ALERT

With the holiday approaching, be on the lookout for spam emails spreading the Storm Worm malicious software (malware). The email directs the recipient to click on a link to retrieve the electronic greeting card (e-card). Once the user clicks on the link, malware is downloaded to the Internet-connected device and causes it to become infected and part of the Storm Worm botnet. A botnet is a network of compromised machines under the control of a single user. Botnets are typically set up to facilitate criminal activity such as spam email, identity theft, denial of service attacks, and spreading malware to other machines on the Internet.

The Storm Worm virus has capitalized on various holidays in the last year by sending millions of emails advertising an e-card link within the text of the spam email. Valentine's Day has been identified as the next target. Be wary of any email received from an unknown sender. Do not open any unsolicited email and do not click on any links provided.

To receive the latest information about cyber scams please go to the FBI website and sign up for email alerts by clicking on one of the red envelopes. If you have received a scam email, please notify the IC3 by filing a complaint at http://www.ic3.gov/. For more information on Internet Crime Schemes & Prevention Tips, go to https://www.ic3.gov/crimeschemes.aspx and https://www.ic3.gov/preventiontips.aspx.

## Phishing Email on Campus

Hi Everyone -

We've seen large number of emails claiming that you need to "VERIFY YOUR EMAIL ACCOUNT" and asking users for information including their user name and password (A copy of the email is at the bottom of this page). The email threatens to have a users account deleted or deactivated if they do not respond. This of course is not true and is an attempt to con you into giving out your personal information. For those of you that do not know this activity is known as 'phishing'. I have reported the emails to CIS and we add the senders to our spam filter as we see them. For more information on phishing you can visit: http://security.tamu.edu/.

Remember that no member of the IT Staff within Mays or TAMU will ever ask for your password.

If you accidentally responded to this email please let us know as soon as possible so that we can take corrective action. Otherwise, please delete the message and move on. As always if you see a suspicious email you are unsure about, we are here to answer your questions.

Thank you to those of you who took the time to notify us that you had received one of these emails and let me know if you have any questions or concerns.

David Jennings
Senior Systems Analyst
Office of the Dean - Mays Business School
Texas A&M University

doj@tamu.edu
440 Wehner | College Station, TX 77843
Tel. 979.862.3950
http://mays.tamu.edu/

Don't be a victim - never give out personal information like passwords, Social Security, bank and credit card numbers in an email!

========== Begin Copy of Phishing Email ==========

VERIFY YOUR EMAIL ACCOUNT

Attention: Web Users,

This message is to all tamu.edu Webmail Web users.

We are currently upgrading our data base and webmail network center to improve

the features of our web service. All inactive email accounts will be deleted,

as we intend to increase storage capacties for existing users and create

more space forregistration of new users (Staff and Students).

To prevent your account from being deleted, we kindly request that you confirm

your account information for update, by providing the information below:

Username : .....

Password : .....

Dept/Faculty: .....

Warning!!! Failure to do this will render your email address deactivated from

our database.

Thanks for your understanding

Warning Code: VX2G99AAJ

tamu.edu Webmail Management

========== End of Copy of Phishing Email ==========