DenverDA
Mitchell R. Morrissey, District Attorney - Second Judicial District
201 W. Colfax Avenue, Dept. 801, Denver, CO 80202
Bus. Phone: 720-913-900
Fax: 720-913-903

Mitch Morrissey
Denver District Attorney

Fraud Alert!!!

Cyber Scams: Beware When Posting Personal Information

Be careful of what you post on social networking websites. The popularity of sites such as Facebook or Myspace is also becoming the primary data source for fraudsters. Although these sites are resourceful ways of keeping friends and family informed, much of what is posted reveals the kind of information criminals are looking for in order to carry out more sophisticated and personal scams. Details one should be wary about posting include names and birthdates of family members, marital status, hobbies, hangouts, addresses, who's on vacation or on a military tour, etc. Vigilance is especially important when it comes to protecting the identity of children. Cyber-scams cover all age ranges, cross all social spectrums, and are often up-dated versions of scams that have been around for a long time. The following are examples of common frauds perpetrated on-line or over the phone based on information obtained through social networking sites:

Grandma Scam: An older person gets a frantic call, presumably from a "grandchild" who claims to have been a victim of a crime or an accident, typically in Canada, or overseas. They need money wired immediately to get out of a jam. Posing as the grandchild, the con artist will give plausible reasons as to why the parents must not be told. These scams are often elaborate - another voice, perhaps a "police officer" or "bail bondsman" may get on the line, will ask the grandparent to verify personal information about the grandchild, then will give instructions on where and how the money is to be wired. Panicked grandparents comply, often wiring several thousands of dollars.

One variation of the 'grandma scam' is the call from a "grandchild" in the military who wrapped up a tour of duty early and wants to "surprise" the parents by returning home. The "problem" is there's no money to do so. Delighted to be "in on the scheme", the grandparents wire the amount that is requested to get the grandchild back home.

Friend in Distress: Yet another and very similar ploy is the "friend in distress". In this scam, a participant of a social networking site receives a message from a site host "friend" professing to be overseas, and in a terrible mess. They appeal to their network friend(s) to wire them money to get back home. Unbeknownst to the network site host,

their website has been hacked and taken over by fraudsters who are carrying out the scam.

Romance or "Sweetheart" Scams: Predators browse social networking sites to seek out on-line "romances". To lure victims, they post eye-catching, but bogus photographs of themselves. Unlike other on-line frauds, sweetheart scams develop slowly and are relatively long-term. Suddenly, the "suitor" is faced with an awful dilemma and needs cash. Perhaps it's a sick child, a terrible accident, or a false imprisonment. Sound familiar? The victim is asked to wire money, or to cash a money order and to send back the cash. A couple of distinguishing characteristics of the sweetheart scam is the suitor's poor use of English grammar, and frequent, over-used expressions of love. Many sweetheart scams originate in Nigeria or Angola, and involve third-party accomplices' in another country, typically England or Canada.

DON'T BECOME A VICTIM!

- Be careful when posting personal information. Keep in mind that prisoners often peruse social networking sites, and can perpetrate a scam from jail.
- Never share detailed information about upcoming trips, military tours of friends or family members, birthdates, addresses, etc.
- Be mindful that photos might reveal too much background information, such as street names or license plates.
- Don't post the full names of children or their friends.
- Always call a grandchild, friend, parents, etc. to verify that they are in fact, safe.
- Don't click on any link or respond to any hyperlink on a networking site. Often, this is how malware or viruses are introduced. Promptly delete!
- Change passwords often, and establish separate passwords for individual sites.
- Check privacy settings on network sites and give careful thought about the personal information others can access.
- Keep virus protection software programs updated regularly.
- A WORD ABOUT WIRE TRANSFERS . . . It's the preferred method used by criminals because money sent over a wire is difficult to trace.

Scams that play on emotions not only result in the loss of substantial money, but are particularly devastating to victims. The inability to stop,or to prove such crimes are all the more reason to take special precautions when sharing personal information with others on-line.

Denver DA's Fraud Line: 720-913-9179

Follow us on Twitter @DenverScamAlert

November 2010