



Arizona Crime Prevention Association

Volume 5 Issue 2

A publication of the Arizona Crime Prevention Association

February 2011

Top Five Identity Theft Scams of 2010

Articles submitted by Brian Kornegay, Phoenix PD

The risk of becoming a victim of identity theft is everywhere. Criminals can gain access to personal information through various ways including mail, computer, credit cards, and even garbage cans. Your BBB has identified the top five scams seeking to steal your identity in 2010.

"ID theft prevention should always be on an individual's mind," said Matthew Fehling, President/CEO of BBB. "When it comes to protecting your identity, an ounce of prevention is worth far more than the amount of money, energy, and agony that goes into getting your life back to normal after your financial and personal information has been stolen."

The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have had their identities stolen this year. Victims may not be aware about the theft until they review their credit card statements and credit reports, or are being contacted by a debt collector.

BBB recommends being on the lookout for the following identity theft scams:

Social-Networking Scam

With the rising use of social networks, ID thieves can hijack accounts and post worrisome status updates, urging friends to send money. Frequently, these messages and status updates revolve around being mugged overseas or being stranded out of state with no money. Friends who read the message immediately grow concerned and try to help by wiring over funds to identity thieves.

BBB Advice: Contact friends and family to speak with them personally about the message received. This will help determine if the message received is legitimately from a friend.

Telephone Denial of Service Attack Scam

Criminals will tie up a phone line with hundreds or even thousands of calls, while they loot bank accounts. As a result, the bank can't contact consumers to verify the transactions being made because of the tied-up phone lines.

BBB Advice: Never give personal information to an unsolicited caller or via e-mail; change online banking and automated telephone system passwords frequently; check account balances often; and protect computers with the use of the latest virus protection and security software.

If you have been targeted by a telephone denial of service attack, contact your financial institution and telephone provider, and file a complaint with the Internet Crime Complaint Center.

Renter's Scam

The renter's scam is also a rising trend. Criminals pose as homeowners listing the personal information of the "real" homeowner asking potential tenants to fill out applications that require personal and financial information, as well as money that is to be sent to an overseas address. The criminal then disappears, leaving victims out of their money and a home, as they realize they were not working with the "real" property owner.

BBB Advice: Always research the property owner thoroughly before providing any personal information and entering into any sort of financial agreement. Never wire money to an overseas address you are unfamiliar with since it will be virtually impossible to recover.

Charity Scam

Criminals pose as legitimate sounding charities seeking to collect money for a particular cause. Many set up fake websites and send e-mails to unsuspecting users requesting sensitive information such as social security numbers and passwords, allowing criminals to steal your identity.

BBB Advice: Before making a donation, remember to review any charity with BBB's Wise Giving Alliance. Visit www.bbb.org/charity to verify that a charity meets the BBB's 20 Standards for Charity Accountability.

Job Scam

Work-at-home scams are conducted by cybercriminals who recruit victims to engage in illegal activities such as money-laundering. Typical scams include e-mails that involve a "you are hired" subject line and specifically target job-seekers. The e-mail, supposedly from the human resources department, will forward new-hire forms that need to be filled out. These forms require the applicant to submit personal information such as one's birthday, social security number, and bank account numbers which cybercriminals can use to steal one's identity. The victim may also be instructed to deposit checks, which are usually fake, and then asked to wire funds.

BBB Advice: To avoid a job scam, research the company thoroughly and make sure you have legitimate contact information. Contact the company directly to verify they are requesting your personal information and never wire any funds.

If you have become a victim to any of these identity theft scams, file a complaint with your BBB by visiting arizonabbb.org or calling 602-264-1721.

*TriValleyCentral.com
Pinal County's Information Source
December 29, 2010*

Are We Reaching the Right People?

For years we have taught people not to give out personal information to anyone who calls claiming to be from a bank or financial institution. We further instruct them that "the banks know better than to ask you for it." How correct is this?

Below is a recent incident; follow along and see how many danger signals you see, and then ask yourself, "Do they really know not to ask for that information?"

A while back my wife received a phone call; I was with her in ear shot of the conversation. The caller said he was calling about our account with a bank my wife and I never heard of before and asked for our account number "to verify" to whom he was speaking. My wife told him that she did not believe we had an account with that bank and even if we did she would not give him the account number over the phone. She asked him what the call was about. The caller said he would not tell her why he was calling until she proved who she was and he was kind of snotty about it. My suggestion to her was to hang up on him. She did not and continued to talk to him.

She told him that even if she would give that info out over the phone, he would need to give her some account information before she even knew what account he was talking about. He said he could not do that and now asked for her social security number. When she refused, he asked for her birth date. Once again she explained she did not know who he was and had never heard of this bank and would not give him that information. Once again I suggest, "Dear, it is a scam. Hang up on him!"

She continues to talk to him and further explains that he called us from some unknown number and we have no way of knowing who he is and if he actually works for the bank.

He now provides a solution, he suggests that she call him back at the number he was about to give her and that would verify he was who he said he was. My wife, now somewhat exasperated with him says, "So

I am suppose to call you back at the number you give me and exactly how does that prove you work for this bank?"

A new story — now he says he does not actually work for the bank, but for a collection agency hired by the bank. She continues to hold her own and again demands more information on this account, as she knows all of our bills are paid up. He will not give her any additional info until she proves she is on the account.

She is starting to get frustrated and I continue with my suggestions to "just hang up on him; it is some kind of scam!!!!"

Instead of hanging up she asked; what is the name of the company he works for again and his name and ID number. He tells her, in a heavy east Indian accent, that his name is George Smith, to which she replies, "Now that is original."

George, not giving up easily, now suggests yet another new solution. He says, "The minimum payment is only \$40 and I will leave you alone." She asks how she would make a payment over the phone. George says that he would be happy to take a credit card number and charge the \$40 to it. She explained to George how ignorant that would be and again asked what account he was calling about. At this point I am *begging* her to please just hang up on him.

But my wife had finally worn George down; he gave up the name of the company which was one of those warehouse membership stores (I will not mention the name). She asked why he said it was this other bank earlier and George explained that the credit account for our membership was through this other bank. He further tells her what we bought and at what two locations (and yes, those are the two stores we visit and exactly what we would have bought) and he gives her the address he has for us. The address is not ours, but it is my mother-in-laws. Now this is getting scary.

We are still not convinced of George's validity, but suspect something bad has happened with someone's account. She explains that she paid the account off in full months ago, has not received a statement

since and suggests to George that we call up the warehouse store to verify his story. George, as expected has a reason why not. He says that the credit account info is handled by the bank he represents and that the people at the store whose name is actually on the card would have no information on the account.

We are still not convinced, but my wife assures George that we will get matters settled directly with the warehouse store. George inquires if we will be calling the store and my wife said, "No; we will go over in person." Finally she hangs up.

At this point I am convinced that either we are the victims of identity theft or George was trying to run a scam on us. We drove to the warehouse store in person to figure it out.

Once at the store we explained the whole story with George to the manager. To our surprise George was correct. The store has no access to the credit account info. They cannot tell how much you owe, if we are current or anything. The manager was concerned about our listed address being my mother-in-laws and the fact that we have never lived there. The one piece of info that the store has access to is our listed address. The manager opened our account and we did not have a legitimate address listed. They had it as "2 Glendale AZ" that is all; no street name listed and missing 4 numbers. We have lived in the same house for 15 years; we opened this account after we moved and the store had no record of an address change and could not explain how our address was erased.

The credit manager of the store placed a call directly to their contact person at the credit company and let us talk to them. Finally we know who we are talking to. They were very nice; she told us our last bill was returned as "undeliverable—no such address" (what a surprise...no real address) and because of that it went straight to collections. She told us what our pay off was and we paid it on the spot. I will give them credit; they agreed to drop late fees and not to report it on our credit, as she was convinced it was clearly not our fault. They still have no idea how the address got messed up.

As I was putting finishing touches on this story, one

of my coworkers got a message on her phone thanking her for opening an account at a local bank. Unfortunately she had not and has refused to use this bank because of some issues she had with them years ago. A short time later she gets a call from the bank advising her that her "new account" is overdrawn. The first thing the bank person wanted to know was — you guessed it — her social security number. My coworker hung up and looked up the phone number for the bank and called them. It turns out that yes, an account was opened and then overdrawn, and yes, the person who called asking for her social security number was actually from the bank. She was last seen by me heading out the door to the bank.

So what is the moral of these stories? Are we teaching the right people? We tell citizens not to give their personal or financial information over the phone unless they know who they are talking to and preferably the citizen made the call to the bank. We tell them that the banks know not to ask them for this information over the phone. But do they really know this? Apparently if they do know this rule, they do not always follow it.

How much time and aggravation could have been saved if George had known what citizens are instructed to do. Something as simple as telling us what account he was talking about, no numbers just the name of the company whose name is actually on the front of the card, not the obscure bank that handles their accounts. At the first sign of concern from the customer, instruct them to call the number on their card or listed on their last statement, not the number the company representative is about to give you.

George gave out almost every signal you would expect from a criminal.

I know George's job is to harass and badger deadbeats into paying their bills, but not everyone is a dead beat. Some of us are victims of computer anomalies.

Next step we need to figure out is how to get this info to George and people like him in the "call center."

PS: I do take some of the blame. We asked the bank lady why they don't call us when stuff like this happens. She told us they do but it is automated and it will not leave a voicemail if no one answers.

Thinking back, I did get a call where a computer voice told me to "...stand by for an important message about your account with" Again, some bank I never heard of, so I thought "I don't have an account with you" and hung up. I don't have time for that crap.