(Approx. 1,357 words)

Scam I Am
by Greg Skalka, President, Under the Computer Hood User Group, CA
April 2015 issue, Drive Light
www.uchug.org
president (at) uchug.org

Scam I Am

I don't like things to slow me down
The web is made to click around
Passwords are a royal pain
There's no room for them inside my brain

My inbox may be filled with spam
But I'm not worried about a scam
Google's tracking helps me shop
My Facebook postings never stop

Hackers will not target me
There are bigger fish in the world-wide sea
My check has bounced - there's no money left
Oh no! I'm a victim of identity theft!

Scams, cons, theft and deceit have been around forever. Just as technology has helped us increase our productivity, it has helped the crooks become more efficient as well. The old scams and trickery have been made easier to execute, while new forms of theft have been developed.

The authenticity of bank robber Willie Sutton's quote about why he robbed banks, "Because that's where the money is", may be in question, but robbers today still go where there are things of value. Now their targets are subscriber personal data at Anthem Blue Cross, credit card information at Target and account information from phishing attempts on individuals through email.

With so many institutions, from banks, retailers, insurance companies, medical providers and even the government holding sensitive information about us and apparently not protecting it all that well, we are all at high risk of institutional data theft, though there is not much we can do to prevent it. For most of us, hiding out in the woods with no legal residence, credit cards or medical coverage is not an option. I have Anthem Blue Cross health insurance, so since their announcement of the loss of subscriber data through a cyber attack, all I can do is take advantage of their offer of free credit monitoring and identity theft protection, and watch my accounts and credit reports carefully. While we can't do much about the institutional data hacks, we can do a better job of protecting ourselves from those threats that target us individually.

There is a strong correlation between crime rates and the proximity to a freeway onramp; access to a highway facilitates finding victims and provides criminals a quick and easy getaway. The connection to the Information Superhighway we get through our computers, tablets and smart phones works in the same way, bringing the potential for crime closer to us. Now financial misfortune can be as close as our inboxes or browsers.

We have all received those ridiculous emails reported to be from Nigerian customs officials, foreign attorneys and even the head of the FBI, asking for help or offering huge sums of money for us to claim. It is hard to believe anyone falls for these scams anymore, yet I still continue to receive the emails. I've also received many emails that appear to be from banks, credit card companies and online services, but are really phishing attempts. These are generated by criminals intent on tricking me into providing them with my sensitive information. A lot of them are easy to spot; they may be from institutions I don't have accounts with, or may have misspellings or other flaws that are a tip-off that they are fakes. I have received some very convincing phishing emails, however. Either by random chance or because the scammers knew I had an account there, I've received emails that appeared legitimate and pertinent to my situation, but after close examination and research, turned out to be fakes intended to scam me.

With income tax filing season in full swing, the media is presently full of warnings about email and phone scams related to the IRS. We hear about all these scams and hacks; hopefully we take these warnings seriously and don't disregard them as things that only happen to others. I'd heard about phone scams where callers try to convince you that a loved one is in trouble and you must send money to help them, but I never considered them a serious threat until someone tried to scam my mother.

A few weeks ago, my mom called our home and asked if our daughter was all right. She then told us the story of the scam call she had just received. Fortunately, she was suspicious and did not get taken. It is not clear if she was targeted specifically by scammers with knowledge of our family situation, or if it was just a random call.

When my mom answered the scam call, a young female voice said “Hi Grandma.” Since she has only one granddaughter, my mom replied “Hi Alli”, so it is not clear the caller knew my twenty-four-year-old daughter's name beforehand.

The caller initially engaged briefly in some small talk, like how have you been and such, but then, either having some knowledge or taking a chance, asked if Grandpa was there. The scam would have been exposed at that point had my father been deceased, but fortunately he was there.

The caller then said “Grandma, I'm in trouble, but you have to promise not to tell anyone else in the family about this. Can you do that, Grandma?”

My mom was getting a little suspicious, but agreed.

The caller went on. “Grandma, a good friend of mine died suddenly and I’m in Virginia for the funeral. Because she was Jewish, they had to bury her right away, so I had to travel on short notice. After the funeral, some other friends and I stopped at a restaurant for a drink before returning to our hotels. I only had one drink, but because I was also taking antibiotics for bronchitis, I hit a street light and knocked it over on the way back.”

The addition of bronchitis to the scam narrative is interesting as it generates sympathy for the caller (she is not just a drunk) and could explain why she perhaps did not sound quite like my daughter. This scam would understandably work best on grandparents that don’t often get calls from their granddaughters. I’m certain my wife and I would have been able to recognize our daughter’s voice had we been called.

The caller continued. “Grandma, I’m at the police station here. They said they would not charge me with anything if I could pay for the damaged street light, but I don’t have the money. A lawyer here is willing to pay for it on my behalf if you can send him the money. Here is a policeman.”

A male voice came on the line. “Hello, this is Officer Raleigh. Your granddaughter needs you to send $2300 to cover the damage to the street light, and then we can release her with no charges. Can you do that?” Officer Raleigh then provided detailed instructions to my mom on sending the money. She was to take $2300 in cash, with two IDs, to a Walmart and send it via Western Union MoneyGram to Ronald Pearlman in Bristol, Virginia. When Officer Raleigh asked if she understood all of this, my mom replied that she didn’t think all this sounded right.

Officer Raleigh put the phone down for a minute, as if he was not sure what to say. When he came back to the call, he began repeating the payment instructions again. When my mom again said she didn’t think this sounded right, Officer Raleigh hung up. The scam was thwarted.

I told my mom’s story to a coworker a few days later and she said a similar thing had happened to her relatives in Mexico, except that it was kidnappers calling to say they had their daughter. Her relatives unfortunately paid $1500 before finding out their daughter had been safe at a friend’s house all along.

With all our personal information entrusted to companies and the Internet, hackers and crooks can have a much easier job deceiving us. To avoid being taken advantage of by these thieves, we all must unfortunately be more suspicious and skeptical. Just because you’re paranoid doesn’t mean they are not out to scam you.