A Recent Scam Experience

By Jeff Wilkinson, President, Sun City Summerlin Computer Club, NV
December 2019 issue, The Gigabyte Gazette
www.scscc.club
Clearmeadows11 (at) gmail.com

Recently I received the “Social Security” scam call, the recorded message informing me that I should call an 800 number because my account was about to be suspended. I decided to play along and see what the suspected scam pitch was; since I was 99.99% sure that Social Security doesn’t call you.

I called the 800 number, exclaimed my surprise that there was a problem and breathlessly asked what the problem was. The responder, “Officer Ronald Smith” explained, in an almost unintelligible accent, that he was a senior investigator and I should get a pencil and paper and write down his name and badge number, which he proceeded to give me. He then went on to outline the “problem” which included seven bank accounts opened under my social security number. He said the accounts had been used for money laundering and an investigation was underway with an arrest warrant about to be issued. In addition, there were multiple credit cards also under my social security number which had been linked to illegal activity.

“Officer Smith” then asked if these were my accounts. Upon my answering No, he explained he needed to know how many bank accounts and their approximate balance and how many credit cards I had and their credit limits. I responded with fictitious information of course. He advised me that this conversation was being recorded and I was repeatedly told to listen to his instructions very carefully. When I told him in a frightened, exasperated voice that the accounts he described were not mine, he wanted the local police department phone number so he could call to see if we could clarify some additional information. I gave him a fake phone number and he put me on hold; he came back a short time later and said that the number I gave him was incorrect!

“Officer Smith” then told me I could get the number from the yellow pages or Google and said he would wait while I looked it up. When I asked why *he* didn’t have it, he exclaimed he did but was not allowed to give it to me. I looked up the number in the city I had claimed to live in and gave it to him; he again put me on hold and returned a couple of minutes later. He said he had a senior investigator on his other line, and she would be calling me. I was to put him on hold when she called. Then my phone rang! The call was from the number I had provided which was the number of the Palo Alto, CA police department! “Officer Smith” told me to put him on hold and to add the new caller to the conversation.

Throughout this entire 22-minute ordeal he had not yet asked for any money or access to my computer. I was tempted to continue the charade, but the language barrier became intolerable along with the level of minutia, so I ended the calls. Almost immediately my phone began ringing from an unknown 800 number, over and over until I blocked the number. I believe the ploy was to obtain my information such as date of birth, address and social security number so they could steal my identity.

Although I didn’t get far enough to determine the full scam, I was very surprised that they added so much credibility by calling me back and “spoofing” (faking the Caller ID) of the actual police department number I had provided and they had checked!! As we know, spoofing a phone number occurs often on junk and scam calls. This specific trick could cause a reluctant mark to falsely think they were maybe being too cautious. The scammer may attempt to retrieve your date of birth, name, address and partial social security number by asking throughout the conversation for you to verify the information. With those items, it is possible to initiate a change of address and phone number with Social Security and then redirect your direct deposit to a different bank.

Having repaired two cases of scammers gaining access to computers that week, one which was able to gain bank information and withdraw a four-figure sum of money from a retiree, I was interested in experiencing the actual pitch. It can’t be stressed enough that allowing remote access to your computer from random phone calls, emails or web page screens is to be avoided. Also do not release any personal information to unknown callers no matter how official they attempt to sound, with so much information available in the public domain many times only a small about of additional information is needed to initiate an identity theft.