

HOW NOT TO GET YOUR LOST MONEY BACK

People in the business of fraud prevention and consumer education knew for many years of the “scam recovery scam”. It’s a fairly rare bird, but not unknown. In this scam, someone loses money in a fraud, it could be anything from a lottery fraud to timeshare fraud. The victim, upset and financially embarrassed, then gets a phone call some weeks later from someone sounding official, often claiming to work with a government agency protecting consumers. The caller will tell the victim, yes, we know about the fraud in which you lost money, isn’t it terrible? But, they continue, we have a solid lead on where your money went, and we can very likely recover most if not all of it. However...this caller will need the victim to invest money in the recovery operation.

All too often, the victim, grabbing at a chance to get back some of the loss, will fork over yet more money, which will disappear. I call this a scam recovery scam.

Today I learned of a clever crook that seems to have married this scam with a popular ongoing scam, the tech support scam. Sally Vanderbleek of Fulton IL told me how it happened to her. Sally somehow downloaded a virus onto her desktop computer. She didn’t know this until one evening, as she reviewed her emails, her screen locked up, started flashing a warning, and an audible alarm started sounding in the computer. The warning told her, someone attacked her computer. Within minutes, she received a phone call from a foreign-sounding man who said he worked with Microsoft. He knew her computer contracted malware, and wanted to fix the problem. He persuaded Sally to allow him to remotely access her computer. The caller showed Sally all kinds of “problems” he wanted to fix. He quoted a price of \$299 to Sally. With her screen flashing and the alarm sounding, Sally agreed to the deal.

The caller instructed her to access her bank account, and create an electronic draft from her account to pay the caller. She did. She also gave the caller her social security number. The caller seemed to correct the problem, and all seemed right with the world. Problem solved. So far this is a pretty standard tech support scam. But we are not finished...

Two weeks later. Sally received another call from the “Microsoft” tech. He told her, his company was forced to re-locate by the Internal Revenue Service. As part of the re-location, Microsoft needed to refund Sally’s \$299. The tech convinced Sally to allow him to access her bank account again, for him to re-deposit the \$299. Instead, Sally saw the deposit of \$2099 to her account, not \$299. The tech asked if everything looked right. Sally told him, no, you deposited way too much money. The tech sounded very agitated and distressed. He said he made a mistake, and needed \$2000 back right away, or his boss ordered him to pay that money out of his own pocket. The tech started weeping and sobbing.

Sally did not want to take anything not belonging to her, so asked how to pay him back. The tech told her to go to Walmart and load \$2000 on iTunes gift cards, then call him back. He planned to transfer the money off the iTunes cards to pay himself. The previous sentence is the only thing true this tech ever said.

Now it was in the late evening, and Sally was not inclined to leave her home and drive eight miles to Walmart. She wanted to do it the next morning. NO! NO! NO! The tech argued with her, do it NOW! At this point, Sally smelled a rat. She hung up and called a relative. That relative told her this sounded like a scam. She needed to go to her credit union when it opened the next day. The tech called several more times that evening, but Sally resisted his pleas.

Next morning, Sally went to her credit union. A credit union officer reviewed her account and saw, indeed, someone deposited \$2099 into her checking account the previous evening – but they transferred that money from Sally's savings account, only giving the illusion she got money back. It was all a shell game, a scam. The credit union closed this account, and even refunded her loss of the original \$299.

Even though Sally turned out financially whole, she suffered a great deal. She told me she became physically afraid of her computer. "I thought for a week someone was going to jump right out of the computer at me", she said. Sally felt as if someone physically attacked her. And the closing of the credit union account and re-opening of another caused considerable hassle with the direct deposits into the account, and electronic payments coming out of the account.

Sally told me she wanted this story shared, and agreed to the use of her name, to highlight the fact she knew this kind of thing happened, but never dreamed it could happen to her.

What's to learn here? The most important thing to know is, never allow remote access to your computer to someone who calls out of the blue. It is always a scam. A close second is to condition yourself on what to do if you contract a virus which causes your computer to lock up, or even sound an alarm. Realize you just got a virus. Don't panic, don't call the "help" number you will likely see on the screen. Call someone you trust, or contact a local computer tech for guidance. Turn your computer off and don't use it until you get some help. Last thing, any stranger who wants you to load money on to an iTunes card is a crook. These cards are very popular with scammers right now.

DEFENSIVE DRIVING CLASS RE-SCHEDULED

Eastern Iowa Community College needed to cancel the defensive driving class scheduled for this week. They re-scheduled it for November 15, 2016.

To register, you can call Clinton Community College at 563-244-7053, the Eastern Iowa Community College District at 563-441-4100, or go online to www.eicc.edu/ceregistration. It is helpful if you know the section number for these classes when you register, here they are:

- Section 174533 - \$20
- Section 174555 - \$15 (for AARP members)

CONTACT SENIORS VS. CRIME

Let me know about scams, fraud, or other crookedness you run across. Most of what I learn, I learn from you. Contact me at Seniors vs. Crime, Clinton County Sheriff's Office, 563-242-9211 extension 4433, or email me at randymeier@gapa911.us

End of column/rmeier