### (Approx. 886 words)

### Fixing a Nasty Computer Hack

David Kretchmar, Hardware Technician
Sun City Summerlin Computer Club
<https://www.scscc.club>

dkretch (at) gmail.com

I recently completed a repair on a club member’s computer after he allowed a “helpful” technical representative, probably from the other side of the world, to remotely access his computer. Unfortunately, the victim in this case apparently failed to read or heed my article in the November 2021 *Gigabyte Gazette* (<https://www.scscc.club/Gigabyte/gg_2021-11Nov.pdf>) warning that these types of scams were becoming increasingly prevalent.

The “bait” in this instance was an official-looking email, supposedly from Cox, stating that the victim had been substantially overcharged on his Cox bill and he was due a refund of $400. The victim telephoned the scammer using the phone number in the email. Next, he went online and downloaded and installed remote access software at her instruction. He then allowed the purported technical representative to initiate a remote access session and log into his system. The victim began to feel uneasy when he saw that things were being done on his computer that had nothing to do with Cox. He finally became alarmed and hung up on the scammer when she asked for his bank account information “to process his refund.”

Unfortunately, this victim did not immediately shut off his computer, so the scammer could continue to mess with his system remotely, I suppose as a departing coup de grace for a failed scam. The victim could no longer access his computer, which displayed the Windows 11 “Gray screen of death” right after he entered his PIN during login. Microsoft has finally replaced its famous “Blue screen of death,” which provided a bit of mostly useless information, with a “Gray screen of death,” which provides no information.

The victim, who runs an online business, called me in a panic. This was especially interesting to me since I have had minimal experience working with pooched Windows 11 machines. I was curious to see if there was a substantial difference in addressing issues in Windows 11 versus Windows 10 (there was not, at least for this user’s issue).

I researched the gray screen issue online and did not find much helpful information. Many writers suggested the problem was bad video drivers or a bad hardware connection. I knew there was no physical issue since the miscreant obviously never had physically assessed the victim’s computer. And I doubted the graphics card drivers were the problem since messing with them would cause an immediate catastrophic system failure, even if it could be done remotely on the fly. After providing answers that did not solve the issue, many sites did offer to sell me their software, which they said would fix the problem. No thanks.

I finally decided to approach the Windows 11 system the way I would Windows 10. Getting past the gray screen of death was straightforward; I booted into Safe mode and repaired the Windows startup. When I finally got into the victim’s computer, I removed the remote access software. Then I did a system refresh, keeping all of his original data files and programs but replacing all of the system files. I wanted to assure the club member that there were no nasty surprises on his system due to his encounter with the scammer.

Yet when I could finally boot to the victim’s desktop, I saw something very strange. The victim’s desktop icons, files, and folders had disappeared. I considered that the scammer could have put the victim’s computer in tablet mode, which messes up the desktop. I learned that Windows 11 does not have a dedicated tablet mode. Again, an online search for the problem was mostly useless. Most writers suggested going to Personalize themes, Icons and checking the icons I wanted to appear on the desktop. This did not address the issue of nothing showing on the desktop, files, folders, and icons. Naturally, many of those offering useless advice online had a software package to sell, which they assured would fix any problems. Again, no thanks.

I found an article that suggested I right-click on the desktop, left-click on View (#1), then make sure “Show desktop icons” was checked (#2). Yes, that sneaky scammer had hidden everything on the victim’s desktop with three clicks of her mouse. However, when I left mouse clicked on “Show desktop icons,” the victim’s desktop appeared normally. This was the first time I had seen a scammer throw two problems onto a victim’s computer.

When contacted, a scammer will often state that to help you, they must remotely access your system. They will try to get you to download remote access software that will give the scammer access to your computer. Just say NO! There are few legitimate reasons someone needs to access your computer to provide assistance.

I mentally divide computer hacks/scams into two categories: tarantulas and scorpions. Tarantulas are big and scary looking, yet their bite is virtually harmless to humans. The most dangerous scorpions are the tiny ones you are likely not to see until they have stung you, and they can send you to the emergency room or at least to bed for a day or two. The unfortunate victim in this story ran into a scorpion that stung him twice. The sting would have been even worse had he allowed them access to his bank account.

