### (Approx. 592 words)

### And the Scams Just Keep Coming David Kretchmar, Computer Technician Sun City Summerlin Computer Club <https://www.scscc.club> dkretch (at) gmail.com

If you’re on the phone with some nice, polite person who asks you to download some software onto your computer that will allow them to remotely fix something that has been a problem, please think twice about it. Then do not do it. The chances are high that you are dealing with a scammer trying to get financial and personal data about you.

A picture containing graphical user interface

Description automatically generatedIt is probably generally a very bad idea to give a stranger access to your computer. Yes, there are exceptions; I have allowed a Microsoft Tech to access my computer remotely to fix an Operating System installation problem. But anything short of that, such as reactivating a permanent version of Microsoft Office after a hard drive failure, did not require me to relinquish control of my computer to a stranger. Therefore, it is extremely unlikely that any issue you might be having would require you to give a stranger remote access to your computer.

## My Experience

A person wearing headphones

Description automatically generated with low confidenceI was having problems installing AOL Gold on a client’s new computer. A Google search led me to what appeared to be a legitimate AOL site, or at least it fooled me. I called the number and spoke to a nice, polite young lady, who might have been on the other side of the world. She explained that to fix the problem preventing AOL Gold from loading, I would have to give her access to my computer.

She asked me to download and install a program that would allow her to access my computer, which I foolishly did. She then sent me a code by text or email, which I had to enter to activate a remote session.

Then for the first time, I wondered, why does she need to do that? I told her I was a computer tech who could probably follow her instructions, and she gave me an unsatisfactory answer. So, I terminated the call and uninstalled the remote access software.

Remote access programs such as TeamViewer, AnyDesk, LogMein, and dozens of others are legitimate programs, but they can be used for nefarious purposes

Scammers expertly reproduce the logos of legitimate software providers, such as AOL and McAfee. They can even spoof their email address, so an email appears to be coming from a legitimate company.

## Fake antivirus email scam

Text

Description automatically generatedScammers might come at you via your email. For example, one message I have seen purports to be from McAfee or Norton, stating that your credit card will be charged for another year’s subscription unless you contact them via a phone number or hotlink in the email. This message sounds authentic to many users, who might have had McAfee or Norton in the past, or who got a free trial that comes with many new computers.

When contacted, the scammer will state that for you to avoid additional charges, the scammer must remotely access your system. They will try to get you to download remote access software to give the scammer access to your computer. Just say no. There is no legitimate reason someone needs to access your computer to remove a program.

As we approach the holidays, computer scammers and hackers seem to step up their attacks on computer systems. Users are especially vulnerable to messages from vendors such as Amazon stating there is a problem with their order since many of us do order gifts from online vendors this time of the year. So don’t let your guard down!

A picture containing person, person, fish

Description automatically generated