

TECH SUPPORT SCAMS – YOU CAN LOSE ONCE, LOSE AGAIN, AND LOSE SOME MORE

Probably the most successful scam I am hearing about right now is the tech support scam. And by successful I mean this scam succeeds in attempts to cheat and steal. From the reports I see, about twenty percent of people getting these tech support scam calls fall for the deception. That's a pretty high rate.

The scam works like this...You get a call out of the blue, almost always from a man with a South Asian or Indian accent. The caller tells you he represents some software or computer company, often Microsoft. He wants you to log on to your computer immediately. He'll give a variety of reasons:

- Your computer is malfunctioning, affecting the entire internet
- Your computer is the target of a malicious hack by foreign criminals
- Your computer is already hacked, and is full of malware installed by crooks

The caller persuades you to go to a website which will allow him to remotely access your computer. He will take control of your computer, and convince you it needs major repair and installation of new programs. And this will cost you. The caller will ask for your credit card, or your bank account information, telling you they plan to charge \$120 to \$250, that's the going rate. So you agree to this, giving up your credit card, or bank account, or sometimes both.

This is all bogus. Anyone calling you and wanting you to jump on your computer right away is a cheat. If you do allow these scammers in your computer, they will fabricate problems which don't exist, and pretend to fix these non-existent problems. Or install useless software to keep up the appearance of doing something. Even worse, they can steal your personal information off the computer, or install malware which can later capture your passwords or other information. And remember, they also have your credit card and bank account information, so they can make bogus charges and withdrawals.

This is all bad enough, but it can get worse. Folks who fall for this the first time seem more disposed than other scam victims for what I call the "recovery/refund scam". With these tech support scams, this takes two forms:

- Scammers continue to contact their victims every couple of months, and offer to sell more worthless programs. This can go on for months or years.
- Scammers contact their victims a couple days after the first scam, and say they screwed up, their "fix" is useless, and you deserve a refund. They will produce a screen which is manipulated to make it appear they are depositing your refund to your bank account

(remember the victim gave away the bank account information). But then they will appear to make a huge mistake, and refund you thousands of dollars more than charged. The scammer will get very emotional, pleading with the victim to return the money. But the only way to return the money is to purchase pre-paid debit cards, usually iTunes, and give the scammers the serial numbers. The “over-payment” refund is fiction, but the victim loses all the money paid for the iTunes cards.

To really compound the damage, anyone victimized by these scam will likely find their computer damaged, loaded with spyware or other malicious software. It will require a clean-up by a real tech, price tag \$60-\$200, if it can be saved at all.

How do we all this bad stuff from happening? Let’s start with that first phone call from a stranger about your computer. Realize it is a scam! Don’t talk to these callers. Hang up. Problem solved. If you do fall for this, you’ll need to do damage control as fast as you can. That means cancelling any credit cards you provided, and closing any bank accounts you gave up. Make a police report. Get your computer checked out by someone you trust. And tell others you know. We need to get everyone educated and bullet-proofed against this scam.

IN THE COURTS

On March 24, 2017, the Federal Trade Commission filed charges against several people and companies for running a deceptive marketing scheme. This scheme involved advertising “free” cooking gadgets or golf equipment on various websites and through TV infomercials. The marketing told consumers these products were “free” or sent on a “free trial”. The seller collected a credit card number “for shipping and handling”. What they did not clearly tell the consumers was their cards would be charged if the consumer did not cancel or return the product. In the case of one product, the seller forced consumers to sign up for more “free trials” by clicking through fourteen more “upsell” pages to conclude the free offer.

This story reminds us to use a lot of caution in signing up for “free” stuff. If it’s free, why do they need your credit card? This is also another reason we need to go through credit card and bank statements line by line. You may see charges originating out of one of these schemes, which you didn’t authorize, or did not fully understand.

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

