DON'T BE A VICTIM OF A CYBER SCAM!

jeff@jeffbohr.com | 239.595.0482

BY JEFF BOHR
Naples Mac Help

These days, it is not uncommon to hear about a friend or family member being taken advantage of every week or two as the internet bad guys get craftier in their methods of fooling the general population. I will tell you how to foil the three most popular cyber scams happening today.

SCAM ONE: *The Phone call from Google/Apple/Microsoft*

Your phone rings and the person knows your name, "Hello Mr. Johnson, this is Michael from Google/Microsoft/Apple calling, we noticed that you were having a problem with your computer?"

This is the hook. At any given time, almost everyone is having some kind of computer issue: email password wrong, printer not responding, documents can't be found, and so on. "What a relief," you think, "help is on the way!"

Wrong! These professionals prey on fear. They will suggest things that may be wrong with your system that they have "detected remotely" and then they continue down that path, eventually getting you to download a small program so that they "can get into your computer and fix this for you," for a low fee from $100 to $750, conveniently charged to your credit card. In reality, they are installing programs that will cause more problems (and more charges) and even deleting files that they will later charge you to recover! Remember that TeamViewer and GoToMyPC are legitimate programs, but when used by the bad guys they are dangerous.

The most important thing to remember when you get a phone call like this is that no one outside your home or office can see what is happening to your computer

> **Remember that no one outside your home or office can see what is happening to your computer unless they are sitting at your desk! 99**

unless they are sitting at your desk! They claim to have access, and by following your lead they create a problem to solve. If you get this type of call, hang up, and do not answer repeated calls back, they will hound you for weeks! If you happen to have given these callers your credit card number, call your bank or card issuer immediately and dispute the charge, they will issue you a new card as well. I have had clients that are very computer savvy fall for the phone call scam, be careful that you don't!

SCAM TWO: *The website 1-800 number pop-up*

This is a common scam that happens without warning and through no fault of the user. A popular website is hacked for a number of minutes, and any visitor during that time will be exposed to a pop-up ad that says "Your computer is at risk! Call 1-800-GET-HELP" so that we can solve your problem!" If you try to close this pop-up, it won't close. If you restart your computer, it comes back. It seems to have taken over your computer, and you are tempted to call. Don't!

Here are sites that will tell you how to solve the pop-up scam:
- *For Mac Users: tinyurl.com/3hf6aedh*
- *For PC Users: tinyurl.com/y8jcac9s*

SCAM THREE: *The Phony Email*

Another common scam is a message in your mail inbox appearing to be from your bank, credit card issuer, airline, or any secure site that you may use. The message may say something like this, and has the appearance of one that is legitimate:

We need to confirm all your account information, you must confirm your account before we close it. Click the link below to confirm your account information using our secure server.

To identify this email as a scam, hover over the address that it appears to be from, in this case, Apple, and you will see the actual sender's address revealed.

As you can see, the address does not contain apple.com and does contain some strange unknown address, delete this message immediately! Do not attempt to unsubscribe from these types of messages, they are also attempting to harvest your personal data.

Know that banks and other online accounts do not send emails asking to verify data unless you have requested a password change or other account change, these do not come out of the blue. Entities now have text message alerts or phone calls to verify activity on your accounts, they do not send emails asking you to log in!

By following these steps, you can avoid falling prey to these popular scams that target your online activity. Remember that no one outside your home or office can see what is happening to your computer unless they are sitting at your desk! If you suspect you are being preyed upon by a cyber stalker, call law enforcement, a family member, or your IT professional immediately for help.