(Approx. 742 words)

Dan's Desk

Don't Respond to Potential Scams

By Dan Douglas, President, Space Coast PCUG, FL

April 2021 issue, *The SCPCUG Journal*

www.scpcug.org

datadan (at) msn.com

PLEASE PRINT THIS OUT AND PASTE IT NEAR YOUR PC AND READ IT BEFORE RESPONDING TO ANY POTENTIAL SCAMS.

Unfortunately, I have seen a dramatic increase in people seeking help after being scammed on their computers. Unfortunately, this includes some of our SCPCUG members. So, this month, I would like to share some precautions you can take to minimize your exposure to getting scammed on your computer.

Let's look at the most common ways of enticing people to fall for these schemes:

1) Phone Calls - Receiving or placing a phone call, supposedly from or to some recognizable, well-known/trusted organization, such as Microsoft, Dell, Amazon, HP, etc.

Prevention and best practices to avoid falling victim:

If you want to contact an organization, go to their official website and click on the contact us link. Do not search for contact info. Scammers pay to be listed first on common searches and will act as if you are calling the real company. I've seen this many times with people trying to call HP for printer issues or supplies. They do a web search and call the first number that comes up, and the person convinces the caller that their printer may need an update, and if they give them remote access, they can check it out, and then it is game over.

It is extremely unlikely you would ever receive a phone call regarding your PC or any activities you perform.

My advice is to immediately hang up on anyone claiming to be calling from one of these organizations.

2) PC Messages - Receiving a screen message on your PC that informs you - take your choice - you have been hacked, you are in danger of losing your banking passwords, your PC has been used for illegal acts and will be reported to the FBI, your IP address has been traced, etc. The message usually states to not turn off your PC and to call some number immediately.

These are commonly delivered through your browser (Edge, Chrome, Firefox, etc.) but can be cleverly designed to hide where it originated from or look exactly like common company messages by using their logos and copies sections from their actual web pages.

Prevention and best practices to avoid falling victim:

Ignore the message – do not be scared or worried. Instead, immediately force your computer to shut down completely (NOT sleep) – pull the plug if you need to. The scammer will usually disable many of the common ways to close the program/browser normally, such as preventing you from clicking on the close X in the top right-hand corner, so forcing the power off may be the only way. Usually, the scam will not permanently infect, corrupt, or access any of your information if you shut it off immediately. Download the free version of Malwarebytes from www.malwarebytes.org if you want to be sure all traces are removed. If you let the scammer have remote access to your PC, you may need to change your accounts (credit cards and financial) and their passwords to be safe.

3) Email – Opening an attachment or clicking on a link embedded within an email can launch any one of many forms of 'attacks.'

Prevention and best practices to avoid falling victim:

The first thing that I always do when I get an email that may be suspicious is to check the sender's email address. Your email program may always show this address, or you may need to hold the mouse over the name to see the actual email address that was used to send the email. Anything that doesn't look normal, such as a domain name that is not the same as the company name, or a sender ID that looks made up, such as dsae12345@ myname.com, I would delete/flag that email as junk and report it as a phishing email. Phishing is where the scammer tries to get you to log on to a website that looks like a legitimate one but really captures your login information – common ones are banks, PayPal, and Amazon. Never open an attachment without checking the sender's email address first. Malwarebytes is a good program that may be able to block many scam programs before they are active if you are using the premium version.