(Approx. 707 words)

Dan's Desk

Tips for not getting scammed

By Dan Douglas, President, Space Coast PCUG

www.scpcug.com

datadan (at) msn.com

PLEASE PRINT THIS AND KEEP 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. This includes some of our own SCPCUG members. This article covers some precautions you can take to minimize your exposure to getting scammed on your computer. First, 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 link to contact us.
* Do not search for contact info.
* Scammers pay to be listed first on common searches and act as if you are calling the real company. I've seen this many times with people trying to contact 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's game over.
* It is extremely unlikely you would ever receive a phone call regarding your PC or any activities you perform on it.
* If you don't screen your calls, immediately hang up on anyone claiming to be calling from one of these organizations.
* Never answer your phone with 'yes.'

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 you 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 they originated from or look exactly like a familiar company's messages by using their logos and copies of sections from their actual web pages.

Prevention and best practices to avoid falling victim:

* Do not click on the message.
* Immediately force your computer to shut down completely (NOT sleep) – pull the plug if you need to.
* Scammers will usually disable many 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 or corrupt or access any of your information if you shut it off immediately.
* If you let the scammer have remote access to your PC, you may need to change your accounts' (at a minimum, credit cards and financial) passwords to be safe.
* Download the free version of Malwarebytes from www.malwarebytes.org if you want to be sure any traces are removed.

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:

* If an email looks suspicious, 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 used to send the email.
* Flag as Spam anything that doesn't look normal, such as a domain name that is not the same as the company name or a sender's ID that seems made up, such as dsae12345@myname.com.
* Report the email as phishing. Phishing is where the scammer tries to get you to log on to a website that looks like a legitimate one but 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.

