LOCAL

Virus holds personal, business computers for ransom

By Cindy Schwarz
The Newsweekly

It's that time of year again: colds, flu and viruses abound.

But, viruses attack more than humans. Computer viruses have names and symptoms. Sometimes those viruses lie dormant in the system until a trigger releases their defective properties.

Keeping your computer safe from these invasive infections, as well as your bank accounts and credit cards, demands pro-active defenses.

Two current, and particularly lethal, computer viruses, whose ultimate goal is monetary by gaining credit card information, are "CryptoLocker" and the one feigning as a "Microsoft helpline" phone call. They have wrecked havoc on local residents and even some businesses who inadvertently opened themselves up to contamination.

"We're getting about 200 calls a month about these viruses and others," said Klaus Schwanitz, owner of Act Computers in the Vero Beach K-Mart Plaza.

He advises that if you ever get a call from Microsoft, IMMEDIATELY hang up.

"Bill Gates and his people are just not going to call—ever," said Schwanitz. "Bill Gates has never called me."

These virus "technicians", call (oftentimes the phone numbers are blocked on caller-ID or come up as 000-000-0000) and introduce themselves as "Mike Smith" or Phil Jones," usually with a foreign accent.

They say they have important information regarding your computer's system and that they've received numerous alerts pertaining to your computer's current performance.

You may be asked, "Have you been getting many alerts recently?"or "Is your computer sluggish?"

If you answer, "yes", the caller immediately delves into how they know this and that they can certainly help, but they need you to go to your computer and type in some information.

By remote, they guide you to access files, in particular ones which will bring you to a bogus site.

The site asks for credit card information. You get to choose: American Express, Master Card, Visa, or others. Don't.

PHOTO BY LISA RYMER

Jurgen and Klaus Schwanitz of Act Computers in Vero Beah receive about 200 calls a month about the newest strains of computer viruses.

If you've managed to get this far—PLEASE hang up before it's too late. It may already be too late for your computer, but regardless, DO NOT give out precious personal information.

"These sites look real. Even we have been taken in by certain bad web-sites when we try to locate computer parts," explained Schwanitz. "It's so unnerving, even for us."

The CryptoLocker virus downloads into your computer and holds your files ransom until you consent to pay to have them released. Fees are upwards of hundreds of dollars.

CryptoLocker can also get into your computer by simply opening seemingly legitimate file attachments in unsuspecting emails.

Then the virus encrypts files. Most often, when the ransom is paid the files are released.

The on-going harm still latent in your computer remains to be detected. So far, researchers haven't been able to completely remove the CryptoLocker virus.

For more information about these computer problems, contact ACT Computer at 772-567-7888 or your own computer specialist.