

## **BELLS AND WHISTLES ON YOUR COMPUTER? MAYBE NOT A GOOD THING!**

The expression “came with all the bells and whistles” usually means you get a product with a great many features and advantages. But in the story I am going to tell you, an eighty-one Clinton widow fell victim to a clever internet scheme which literally featured bells and whistles, which drove our victim head-first into the scheme.

Our victim, let’s call her Maureen, contacted me this week. She owned a nice laptop computer. She told me she had limited experience with the internet. She mostly used it to pursue her crafting hobby, keeping in touch with others interested in her hobby.

On Monday, Maureen decided to check the weather in Atlanta, Georgia, where she knew a relative went for a visit. Maureen knew enough about the internet to type in a basic search in a search engine for weather. The search gave her several websites to check. She randomly chose one, and opened it. Immediately, her laptop sounded a loud, shrill alarm, and a pop-up message covered the screen. The message told Maureen, in frightening language, not to touch anything on the computer that she contracted a virus, and she needed to call a toll-free number for support immediately. And Maureen could not get the alarm to stop sounding, nor could she get the message to disappear. In desperation, she called the phone number. A man with a strong Indian accent answered. He called himself a Microsoft online expert. He assured her, he could fix the problem. He persuaded her to allow him remote access to her computer. In Maureen’s words, “he walked me through it”.

Once this man gained control of the computer, he told Maureen she had a lot of problems, and said it would cost to fix them. He offered her a maintenance agreement for \$380, but refused to take a credit card. Instead – and this is new to me – he wanted to draft her checking account using an electronic check. He persuaded her to type in her name and bank account number. On the screen in front of her, he created a document for her to sign. It looked like the size of a real check, and the man wanted Maureen to use her fingertip to trace her signature on the document. At this point, luck came into play, as one of Maureen’s children came into the room, heard the conversation, realized something bad was happening, shut down the computer, and hung up the phone.

This was a pretty clever and elaborate example of a tech support scam. Maureen needed to close her bank account, since this crook knew her account number now. Maureen admitted, "he was looking in my computer for a long time", so we don't know what other information he saw, or whether he installed spyware or something else to cause Maureen problems later.

Maureen let me look at her laptop. I saw the scary message and heard the very loud alarm. I duplicated the exact search she did on Monday which got her into trouble, and we found the website which got her into trouble. Fortunately, we saw the search engine posted a warning to anyone wanting to visit this site, telling any viewer of the crooked activity associated with this site.

If you use the internet, you need to know some websites can download these kinds of malicious message viruses to your computer. The "conventional wisdom" held that internet users who viewed pornography sites, celebrity gossip sites, or visited sites offering free stuff, were most at risk. I am not sure that was ever accurate, and am less convinced of that now. You should know how to react if it does happen. Here's my advice:

- Keep your anti-virus software up to date
- Don't panic. Do not call the phone number displayed in the message. It is always a scam
- Know how to silence the speakers on your computer.
- Shut down your computer, or even unplug, to interrupt any process underway by the crooks
- Be prepared to take your unit to a local tech for exam and de-bugging. Don't be reluctant to call someone for advice, just don't call the crooks

Maureen says the most important thing is "don't panic, don't be afraid."

## **SCAM TRENDS**

Four people called me in one day to report the exact same scam. Each of the callers used a cell phone. Each received a text message which looked like an email. The message informed them, an uncle died and left them "9.8 gbp". The message told them to reply to another email address for details. This left all four of my callers scratching their heads.

This is an example of a phishing scam. Phishing happens when someone sends out a message designed to pique curiosity, or scare someone enough, to provoke a reply or response. I see it much more often with emails, rarely with text messaging, but it did happen. I conducted a quick Google search which showed "gbp" is an acronym for British pounds, the currency of the United Kingdom of Great Britain. That should give us a clue on where this particular scam originated.

### **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](mailto:randymeier@gapa911.us)

End of column /rmeier