

Be alert to a computer scam

CHRISTOPHER WIGGINS

Anybody who has a computer connected to the internet is vulnerable to be infected with a computer virus. However, the risk of having a computer virus is low as long as one has anti-virus software that is current, but the computer virus is nothing compared to a new more subtle threat that, according to Jeff Fritz, who works in the Verizon Fraud Control Department, "is a severe problem," and that begins with a simple phone call.

A scam making the rounds now, including in King George County, involves receiving a phone call from an "unknown number." The caller identifies him or herself as working for "Microsoft Windows," and states that your computer has been sending signals to Microsoft allegedly alerting the company that there is a major security problem with your computer.

The caller is very friendly and sounds very knowledgeable about computers and uses terminology that is very convincing. The caller asks the victim to launch the 'Run' command and enter a series of keystrokes which bring up windows that show what appear to be warning icons. The caller continues to gain the victim's trust by asking them what they see on the screen. Once the victim responds, the caller says to the victim that this is a serious problem—however, this is misinformation that is disguised as evidence that something is seriously wrong with your computer. After a few more instructions to enter keystrokes that bring up more windows, that to the non-expert would appear as alarming, the caller then says that it is imperative to log onto the website www.logmein.com. The scammer then provides a numerical code to enter into a field on the site and upon clicking submit, the scammer immediately takes over the victim computer and locks the user out. At this point, any information on the computer, including bank account information, passwords to e-mail accounts and social networking sites, as well as any other personal information is at the scammer's disposal. At this point, the unassuming computer user is likely a victim of identity theft.

King George County Sheriff Steve Dempsey said that he is aware of this scam and that it has been reported in the county.

"Microsoft will not call you and ask you

any questions," he said. He added that everyone should be skeptical of any phone calls that request information or that elicit access to people's computers. His advice was to just hang up the phone.

Dempsey said that it was not a crime to call and lie about who these people are and direct computer owners to follow directions they are given, however, once the scammer gains access to a person's computer it becomes a crime and the severity of the crime increases to computer trespassing and the charges and penalties increase depending upon what information is compromised and how it is used.

According to the Better Business Bureau, the company LogMeIn, Inc., which is based out of Woburn, Massachusetts, is a legitimate enterprise with a "B" rating.

Tim Patterson, an employee of LogMeIn, said that the company is aware of the scam and that its remote control services have been used to infiltrate defenseless, unknowing victims. Patterson said that anybody who is targeted or believes to be a target should report the incident to LogMeIn.

"We are tracking these cases," he said. He added that if you're given a code for the logmein123.com site and inform the company, it will trace, locate and ban the user from its site.

Craig VerColen, Director of Corporate Communications for LogMeIn, Inc. explained that his company's software, particularly the 'LogMeIn Rescue', which is the online site the cyber criminals are using in this scam, is legitimately being used for remote software support solutions by tens of thousands of legitimate businesses, "...including 50 of the world's top telecom companies."

VerColen continued: "When we've received reports of abuse in the past, the majority is tied back to fraudulent trials of the software - they are using a trial version of the software, not a paying customer account," VerColen said.

"Use of this software or any of our products for nefarious or illegal purposes - even trials - violates our terms and is immediate grounds for account termination -- it is something we take very seriously. To protect consumers, we've increased aggressive proactive and reactive approaches, ranging from changes to our product and trial process to investigating and taking action on reports of improper use. These investiga-

tions can and do include working to assist legal authorities. But education is equally important."

Katie Hamachek, a spokesperson for Microsoft said, "Our advice is simple; treat callers as you would treat strangers in the street - do not disclose personal or sensitive information to anyone you do not know."

Hamachek went on to state, "Unfortunately this is not the first scam of its kind, and it's unlikely to be the last. The best way to avoid becoming a victim is by being aware of the threat. You should also ensure the copy of Windows you are running is genuine and fully up to date, while ensuring you have installed legitimate software will guard against viruses, spyware, and other malicious software."

LogMeIn company spokesman, Bill Baker said, "people should treat their computer the way they treat their house or their office, meaning: you would never let some random person who shows up at your front door, claiming that there is a problem with your TV, into your house, so why would you do the same with your computer?"

Baker continued: "LogMeIn Rescue is a permission-based tool used by support personnel worldwide to help diagnose and manage remote computers. The only way someone can get access to a computer via LogMeIn Rescue is if the owner of that computer grants them permission. If the owner of that computer did not initiate the support request, then they should not be granting access to their computer to anyone."

Lindsay Goodwin, a spokeswoman for the FBI said, "As with all scams, we ask that citizens remain educated and aware."

She added, "If individuals have reservations about any phone calls or emails they receive, we ask that they report such suspicious activity to the internet Crime Complaint Center (IC3) at www.ic3.gov."

Goodwin stressed that resources are available online through the FBI website. "For further information regarding internet and computer safety, please visit www.fbi.gov," Goodwin said.

Other resources on how to safely use remote access software such as LogMeIn can be found on the company's website as well. Likewise, Microsoft provides education and support materials on its website to help computer users stay safe on the Internet and not succumb to this type of scam.