Keystone
TECHNOLOGY CONSULTANTS

Cybersecurity Tips and Reminders

This Month's Focus- Beware of Scareware!

Below is a classic example of Scareware. This malicious software is used to scare the user into calling for help due to their fake problem. The telltale sign that this is fake is the tech support phone number. Do not trust tech support from unknown entities.

If you have a computer problem at work, call Keystone. At home, call the most tech savvy friend or family member you know. Scareware may also include loud alert noises from your computer speakers. The pop up will not go away by simply closing the internet browser. Logging off the computer session and then logging back in will typically makes this pop up go away.

Send me more info

Be Suspicious. Something is not Right.

These often occur when the user accidentally mistypes a webpage address. Hackers know people will commonly go to any number of websites and will create these scareware sites that live where the mistype occurs. The site lives at goggle.com as opposed to google.com. Also, creators of these scareware pages will make sure their site looks like something similar to common internet search results. Example, user searches for “Java download” and somewhere high in the search results, a scareware site shows up as something appearing to be a source of a Java download.

You may ask, what happens when someone calls that number? Unfortunately, I have seen the result a number of times. The victim calls and a friendly person answers saying they saw the detection and are glad the victim called for help. They ask the victim to allow them to remote in for damage assessment. At this time, their remote control software is installed until someone removes it. They generate fake virus and error reports. They tell the victim they can help fix the problems for a small fee (typically $100 -$300). They then get the credit card info which quickly is sold on the black market. They tell them their problem is fixed and say they are going to disconnect. Their remote-control software gives them persistent access to the computer. They gather as many saved usernames and passwords as they can. They use keyloggers to then gather more usernames and passwords as the victim logs into accounts. They download documents in hopes of gathering sensitive information that can be sold. After they have gathered as much valuable info possible, they may even launch ransomware to encrypt the victim's computer and hold the computer data ransom. In the end, it is a nightmare if a hacker gains persistent remote access to a computer.

Bottom line, never call these numbers for help. Follow the steps noted above and remain skeptical and careful as you search the internet.

Any Questions?
Please respond to this email if you have questions, comments, or desire more information.