

Internet of Things (IoT)

The Internet of Things is upon us. So what does this term mean? In the beginning of the Internet desktop computers were connected to the Internet. This is how you searched for websites and sent email. Then laptop computers came around, then later smartphones and tablets were all connected to the Internet. Now we have cars, security cameras, webcams, digital video recorders (DVR), video doorbells, smoke and carbon monoxide alarms, crock pots and even refrigerators all connected to the Internet. That is why the industry is calling it the Internet of Things, all things can potentially be connected to the Internet.

On October 21st hackers used a Mirai virus to attack a company on the backbone of the Internet. This company called Dynamic Network Services Inc. (Dyn) on the east coast was hit with thousands of devices all sending it messages at the same time. The virus hacked into devices on the Internet and used them to send messages to Dyn. When too many devices try to contact one company at the same time this can bring down the company so no legitimate communications can get through. When too many devices all try to contact the same service at one time this is called a *Denial of Service* (DOS) attack. When Dyn was hit with all these requests it was no longer able to provide its basic service and many people on the East coast were not able to reach websites such as *Netflix*, *Twitter* and *The Wall Street Journal*. It lasted for only part of one day but that was enough for alarm bells to go off.

See <u>The Dyn DDOS Attack And The Changing Balance Of Online Cyber</u> Power.

On Oct 26 the FBI sent a bulletin to private companies warning that this is only the beginning, putting every company on notice that they will be responsible for protecting their products and services on the Internet.

See FBI: New Malware to Spur More Large-Scale Cyber Attacks.

For example a company that makes webcams that was part of this Mirai attack has agreed to pull their devices off the market until a software patch can be issued.

See Webcams used to attack Reddit and Twitter recalled.

So what is our part in all of this? This is a good reason why we need to perform all security updates on our devices. Also, we need to make sure that we are not still using default user names and passwords for our devices. The next time we have an appointment have me take an inventory of all your electronic devices and look and make sure that the devices in your home that are connected to the Internet are up-to-date and are not still using the default user name and password that came from the factory. This will at least stop viruses from using your devices for DOS attacks.



Indian scammers caught

IRS Scammers Caught

Last month federal authorities caught 52 people in the US and India who were part of a scam to call Americans posing as IRS agents and demanding payments. Over the years many of my clients have received such a phone call and have asked me if it is for real or not. Again I am warning everyone that if anyone calls you on the phone claiming to be from the IRS, Microsoft or another organization, just hang up on them. These calls are meant to scare you into giving them money so the safest thing for you to do is to do nothing. Just hang up on them.

More Information

Authorities Arrest 52 IRS Tax Scammers from India and the US

<u>Indian police break up tax scam that may have cheated Americans out of</u> millions

The Internet of Things

Denial-of-service attack

Newsletter Archives

Click here to read some of my past newsletters.

Some of my clients do not realize that my business has expanded to all mobile devices. In fact, any consumer electronic product that you can purchase I can help you with. So if you would like help setting up or syncing your new smartphone or tablet or connecting your new WiFi TV to the Internet, just let me know.

Claude Kerno

Computer & Consumer Electronics Consultant 719.650.9916 claude@kerno.biz - www.kerno.biz