kerno.biz LLC **October 2017**

KRACK WiFi Hack

Most of us use WiFi (wireless technology) everyday and don't even think about it very much. If we have a wireless router in our home or business it is sending out a wireless signal that our devices connect to. At first it was only our computers that connected to our wireless networks but the list of devices grows every day. Many homes have multiple devices such as:

- Computers
- Cell phones
- Tablets
- Streaming boxes (*Amazon FireTV, Roku, Apple TV*)
- Home Speakers (*Amazon Alexa & Echo, Google Home, Sonos*)
- Smart TVs (TVs that connect directly to the Internet for streaming)
- Smart plugs (turn lights on & off)
- Smart thermostats (turns the heat up when you get close to home)
- Smart locks (open doors remotely if say you are at work and a worker comes to your home and you want to let them in)
- Security cameras

and more...

Since 2004 we have setup the wireless router to use WPA2 security which is pretty tough to crack. But now a researcher has found a vulnerability in the way devices "handshake" with the wireless router meaning that a hacker could intercept the communication and gain access to our wireless network.

KRACK Logo

Know as KRACK (short for Key Reinstallation Attack) a hacker would need to be in close proximity to your home or business (within the wireless range of your router) in order to gain access to your wireless network. Because of the relatively short range of wireless routers this limits the vulnerability to only those people that are close to our routers. So for most of us this is not going to be a issue.

What Can Be Done?

Don't Panic

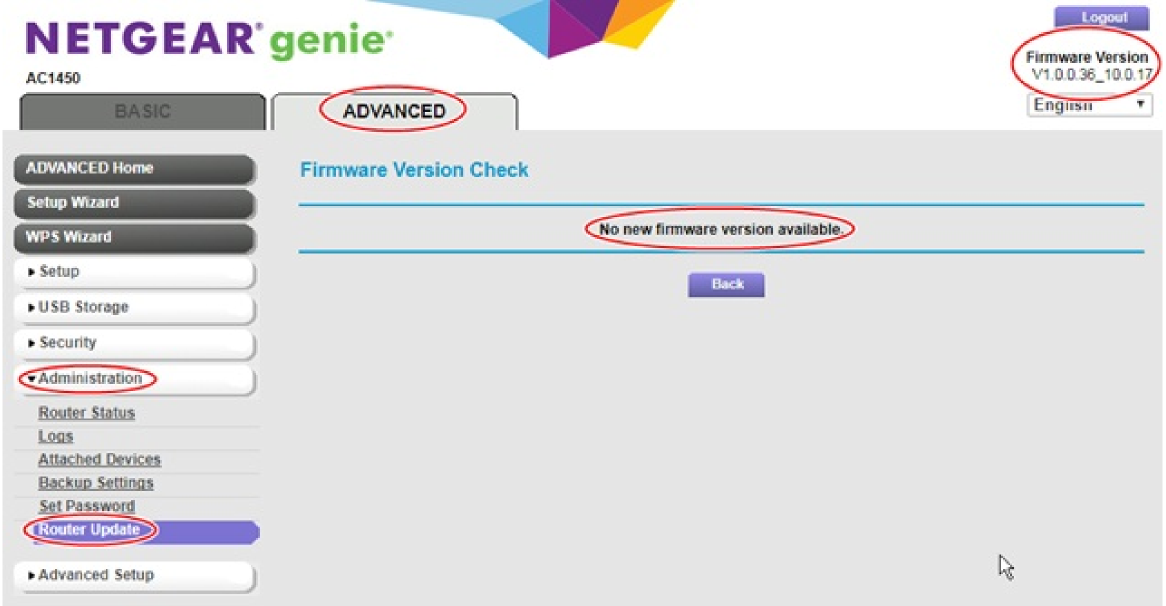
First of all, don't panic. A hacker would have to be in close proximity to your wireless network and have the wherewithal to gain access to your network. Most of your neighbors are not going to know how to hack into your network. But if you are concerned read on for steps you can take to protect yourself.

> "Most current versions of *Windows* and and *iOS* devices are not as susceptible to attacks, thanks to how *Microsoft* and *Apple* implemented the WPA2 standard. *Linux* and *Android*-based devices are more vulnerable to KRACK."

Update Device Software

Really the only thing we can do is install software updates for our devices as they become available. For example, *Microsoft* released a *Windows* update on October 10th that fixed the problem. So all of our *Windows* computers that have automatic updates turned on, this problem has already been fixed. But many other vendors such as *Apple*, *Google*, *Amazon*, *Verizon*, *Comcast*, *CenturyLink*, *Linksys*, *Netgear*, etc. are still working on updates to their devices. And when these vendors do release a software update it is not an automatic process to update the device. Unfortunately, updating the software in electronic devices often requires technical skills beyond the scope of everyday users. This is something that we can put on the list of things to do when performing routine maintenance.

> "*Windows* customers are already protected if they installed software updates released last Tuesday. *Apple* said it's finalizing patches for *iOS*, *MacOS*, *WatchOS* and *TVOS* that will be available in the next few weeks. *Google* said it's aware of the problem and will be releasing any patches necessary in the coming weeks. *Amazon* is also looking into what patches are needed. Router manufacturers *Linksys* and *Netgear* both said they're aware of the problem; *Netgear* has begun putting out patches. *Samsung* products are at risk, and the company hasn't responded to requests for comment on when updates will be available."



Netgear Router Firmware Upgrade Example

Use a VPN (virtual private network)

If you want to take steps to protect everything you do on the Internet you can install the software for a VPN connection to the Internet. Basically a VPN connection is an encrypted connection so no one can see what you are doing. In my April 2017 and January 2016 newsletters I talked about VPNs, what they are and how to get one. My current favorite is *VPN Unlimited*, $49.99 for a lifetime subscription from StackSocial. (**Caution**: I have found that in theory a VPN is a good idea, but in practice VPNs can slow your connection to the Internet, and intermittently, jam up and stop your Internet connection altogether. So although I would like to recommend a VPN to everyone, using them has caused problems with Internet connections and ultimately frustrated the user, so they are only really good in specialize cases with sophisticated computer users who are very concerned with what they are doing on the Internet and can get around VPN troubles.) If you decide you want to try a VPN let me know and I'll help you set it up.

More info:

cNet - KRACK in Wi-Fi security: Everything you need to know

cNet - KRACK Wi-Fi bug: Here's how to protect yourself

cNet - KRACK attack: Here's how companies are responding

WiFi is broken - here's the companies that have already fixed it

TechCrunch - Microsoft already published a KRACK fix, Apple and Google are working on it

VPN Unlimited Lifetime Subscription from StackSocial

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