To all M&H clients,

As you may have read over the past 24 hours, the current industry standard for securing wireless networks (WPA2), has been found by researchers at the University of Leuven in Belgium to have a serious security flaw.

This flaw is not device specific, and is a security issue in the wireless protocol standard itself,. This means that any device (phones, routers, internet enabled devices like security cameras, etc) using wireless is susceptible to the issue.

The good news is that this flaw cannot be exploited remotely, and requires the hacker be physically present within the wireless range in question.

For detailed information here are some resources:

https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability/

https://techcrunch.com/2017/10/16/heres-what-you-can-do-to-protect-yourself-from-the-krack-wifi-vulnerability/

Manufacturers of any device utilizing a wireless connection are currently in the process of upgrading software and firmware to secure their products. This would include, but is not limited to: routers, wi-fi extenders, laptops, phones, and tablets. **The speed at which these devices will have security updates available is manufacturer dependent.**

The staff at M&H Consulting is working hard to remain updated on the status of this security vulnerability. As a client of M&H Consulting, please be aware of the following:

1) **For our clients utilizing our TFAD (Tech For A Day) service, we will be updating router firmware (and other software/firmware as appropriate) during our next scheduled visit.** If your TFAD visits are not frequent enough for you to be comfortable with the time frame (quarterly visits for example), and you would like a technician on site sooner, please reach out to support@mhconsults.com or call us at 866-964-8324 to schedule an appointment. Please also keep in mind, that depending upon the manufacturer of your equipment, updated software/firmware could take anywhere from a few days to a few months before it is available.

2) **The fixes required for this vulnerability are not relegated to just wireless routers.** It is important that businesses with employees accessing email from handheld devices also invest in regular updates to those devices. Clients are advised to include those handheld devices under the normal Tech For A Day program. When our technician is on site for the regularly scheduled visit, please be sure to speak with them in regards to which handheld devices are accessing company email or other data.

3) **Clients who do not utilize our TFAD service should consider reaching out to us to schedule a visit to mitigate this security issue.** If that is not possible, it is important to research this vulnerability and its associated fixes on your own to secure your wireless networks.

4) **This security flaw is not limited to business wireless.** If you would like to ensure your home wireless is also secure, M&H Consulting can work with you in this regard. You may also want to reach out to your internet provider, although they are likely inundated with calls and already in the process of working on fixes. Those planned fixes may or may not be effective for your home network, depending upon your internet provider, their update protocols, the age of your wireless router, and whether or not the wireless router is included in your package with them.

Thank you all for your attention in this matter. If you have any further concerns or questions, please do not hesitate to reach out to our staff.

The M&H Consulting Team.