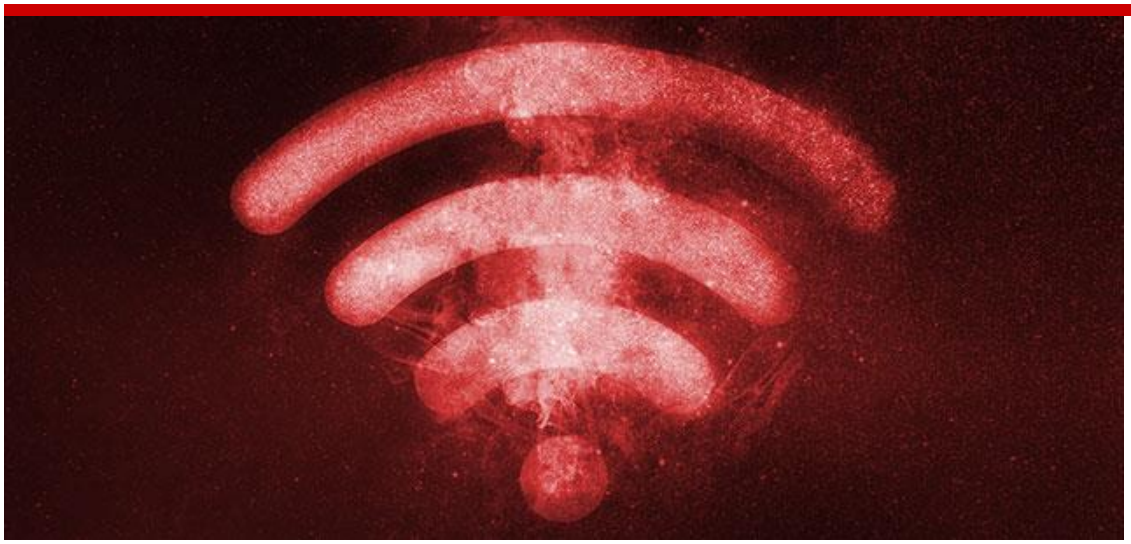
October 17, 2017

www.savvycybersecurity.com

KRACK Wi-Fi vulnerability: What you can do now



Dear Savvy Advisor,

A new, serious Wi-Fi vulnerability that affects nearly all wireless networks was announced by security researchers this week. The attack, being called KRACK, allows hackers to perform wireless network identity theft via a flaw in WPA2 Wi-Fi settings.

The KRACK vulnerability allows wireless networks to be duplicated giving hackers an unencrypted view of anything flowing between your device and the network. For example, if you log in to your email while your network is affected the hacker will be able to see your username and password as well as anything you send while connected.

WPA2, or Wi-Fi Protected Access II, is considered the most secure setting for wireless routers—meaning the majority of networks currently have this setting in

place and are at risk.

The good news is that in order to hack your network, attackers would need to be in physical range of your Wi-Fi network. In addition, sites that are protected with Secure Sockets Layer (SSL) encryption can't be intercepted by hackers. You can determine if a site is protected if the URL in your browser begins with HTTPS://. (Keep in mind, however, that often these security certificates are not configured correctly and many may not actually be secure.)

So far there have been no reported exploits of this flaw, although experts say that businesses are more likely to be targeted than consumers. Here are some things you can do to protect your network from this attack:

1. Update your devices

Microsoft Windows released a patch for KRACK and you should update any Windows devices immediately. While this patch will not fix your router (those vendors will release separate patches when they are ready), it will protect your wireless Windows device from being exploited itself. You can download the appropriate patch for your Windows device here.

Apple has released a patch for iOS in the latest beta version of iOS 11.1. You can download the beta version online but it is not finalized yet and you may experience some issues. The finalized patch will likely be released to the general public and auto-pushed to your devices within the next few weeks.

Google will release a patch for the KRACK vulnerability on November 6th. It could, however, take months for each Android manufacturer to release the patch for its devices.

2. Turn off your office Wi-Fi

If you currently use a wireless connection in your office, we recommend turning it off and sticking to a wired Internet connection until router patches are released. With your Wi-Fi enabled, a hacker could possibly sit in your parking lot and dupe your network to intercept and download data shared on your network—including client information.

3. Check your router manufacturer for updates

Most router manufacturers are currently working on KRACK patches for its models. Charged blog is currently keeping a list of firmware patch status for most routers

and devices. You should also check your manufacturer's website for updates.

Once a patch is released for your router, you will have to update the firmware. This can be a complex process so you may want to ask your IT specialist for help. You can also refer to these instructions for help.

Newer routers come with apps that make updating your router firmware less difficult. You may consider upgrading to one of these new routers in the near future.

Once your router is updated, you can turn your Wi-Fi network back on.

4. Stay tuned

The KRACK vulnerability is a developing story and more news is likely to come out in the following days. We will continue to update you as more information is known.

As always, feel free to send questions to cyber@horsesmouth.com.

Best,

Sean M. Bailey
Editor-in-Chief
Horsesmouth

Devin Kropp
Associate Editor
Horsesmouth