Here’s What You Need to Know About KRACK, the Worst Cyber Threat Yet

November 2, 2017

 by Jim Akin

Chances are, you’ve got passwords to at least a handful of Wi-Fi networks saved on your smartphone, tablet and laptop. Most of us do, because wireless Internet connections are central to most homes and workplaces.

That’s why a recently uncovered security vulnerability known as KRACK is so significant. It puts the private data of virtually all Wi-Fi users at risk. Here’s some background on the extent of the issue, and guidelines on what you can do to protect yourself and your data.

What is KRACK?

KRACK is a clunky acronym for a criminal hacking technique (Key Reinstallation AttaCK) that can expose information shared on Wi-Fi networks, even over connections “secured” with data encryption and passwords.

Without delving into the technical specifics, (there’s a good detailed take here if you’re curious), the vulnerability breaks WPA 2, the strongest and most common form of encryption used to protect data on home and business Wi-Fi networks. WPA 2 encryption is designed to maintain private connections so that anyone who hijacks data by “listening in” to a wireless-networking signal without your password (and the permission that implies) receives only unintelligible chunks of information. KRACK can thwart that, exposing credit card numbers, account usernames and passwords, and other private data that could end up on the dark web, for any criminal to abuse. In certain instances, KRACK can even enable crooks to install malicious code on devices and websites. (See also: What to do if you are infected with malware.)

Who’s on KRACK and what can be done?

Because KRACK affects industry-standard Wi-Fi security, and not just a specific web browser, app, or operating system, it affects all kinds of Wi-Fi-capable devices. Devices running every kind of commercial operating system—MacOS, Windows and Linux computers and laptops, Apple iOS and Google Android smartphones and tablets, etc.—are all susceptible.

Sealing the KRACK requires individually updating the software on every device, and unless you have an IT department at your disposal, it's on you to make sure those updates happen. One way is to enable automatic software updates on your device – a good way to ensure you always have the latest security fixes.

Many of the updates needed to correct the KRACK vulnerability have already been delivered, but others are still in the works:

- **Windows computers**: Windows security updates issued October 10, 2017 patched the KRACK vulnerability. The Windows Update function on your computer can ensure you've got the necessary patches in place. (Click here for Microsoft's security upgrade guide.)
- **Apple iOS devices** (iPhone, iPad and iPod): On October 31, 2017 Apple released an update, iOS 11.1 that patches the KRACK vulnerability on supported devices. Older Apple phones and tablets that can't run iOS 11 may remain vulnerable.
- **Apple MacOS devices** (iMac, MacBook, and Mac Pro): The MacOS 10.13.1 update issued October 31, 2017 corrects the vulnerability. Devices running older versions of MacOS may still be at risk. (Click here for information on Apple's KRACK patches for various devices and operating systems.)
- **Phones, tablets, and Chromebook laptops running Android 6.0,** estimated to be more than 40% of all Android devices, are at risk. Google, developer of the Android operating system, told technology website The Verge it expects to issue a KRACK security fix for its own Pixel smartphones by Nov. 6. The timeline for other Android devices hasn't been spelled out yet.
- **Home and office Wi-Fi routers:** The wireless networking devices in your home and office may need to be updated to correct the KRACK vulnerability as well. Manufacturers will be issuing updates individually, so you should check with the maker of your hardware to see if and when it will be providing a fix. The technology-news website ZD.net is maintaining a list of device vendors and their KRACK-update status that may be a helpful resource.
- **Smart-home appliances and devices:** Smart assistants, wireless camera and audio systems, smart TVs and other appliances known collectively as the internet of things (IOT) all use Wi-Fi connectivity, and are potential targets for KRACK abuse. Amazon and Google have announced that they are working on updates for their respective voice-controlled assistants, Echo and Google Home, but among major IOT vendors, so far only Nest Labs (a sister company to Google) has released fixes for its products. For other IOT devices, consult the manufacturer's websites for update information.

Until you can install these fixes, consider turning off Wi-Fi on your portable devices. Depending on how you use the Internet, that may mean significant increases in data usage (and potential fees) on mobile devices. It might also mean tethering laptops to old-fashioned Ethernet cables at home, work and in hotels. That may feel extreme, but it's the only sure-fire way to guarantee you won't be exposed to KRACK attacks.