Researchers Discover a bug in WiFi Encryption

Posted At : October 30, 2017 2:54 PM | Posted By : Admin
Related Categories: Security, Wireless

Nearly everyone with a laptop, "pad" or smartphone regularly uses public and private Wi-Fi access points. Many have what's called WPA2 Security on them. We all dutifully setup a relatively complex password to get on these WiFi systems. Once done, our machines automatically connect to these networks when we're in range. Perfect, easy, and secure - well not quite.

Several months ago, a vulnerability in WPA2 was discovered. Most of the big guys (Microsoft, Apple, etc.) quicly patched their operating systems, some even before the WiFi access point manufacturers. If your systems were automatically updated, you were likely fine. The non-technical press recently caught on to what's been going on and the articles started flowing and so did the phone calls and emails to us about the condition of clients WiFi systems.

This article from the FTC does a good job of reviewing the issue in a non-technical fashion. Be cautious as always about how you access WiFi networks, particularly public ones.

You've read recent news stories about a vulnerability discovered in the WPA2 encryption standard. (Some reports refer to it as KRACK – Key Reinstallation Attack.) Should this be of concern to your business? Yes. Does it warrant further action at your company? Absolutely.

If you or anyone at your business uses a smartphone, laptop, or IoT device connected to a Wi-Fi network, the information sent over that network could be at risk. **Researchers have found a bug** that lets attackers "break" WPA2 – the encryption that protects most wireless networks – leaving data you send exposed.

The bad news is that this isn't just a problem with a specific device or manufacturer. It's a problem with the encryption standard nearly all Wi-Fi devices on the market use to scramble communications, prevent eavesdropping, and deter tampering. The upshot is that if anyone at your business uses a device to connect to a wireless network at work, at home, or on the road, this bug means they can't rely on that connection being secure.

The good news is that the bug can be fixed with a security update or patch. Device manufacturers and software companies are aware of the problem and updates are rolling out now. Keep an eye out for authorized fixes from your device or software company.

In the meantime, connections other than Wi-Fi (like your smartphone's 4G/3G carrier connection or a connection with an Ethernet cable) aren't affected. So consider using them instead of Wi-Fi until the updates are available.

Even so, this bug is a reminder that there's no single solution to secure your data, and all of the other tips for protecting your sensitive information and security online are more important now than ever, including:

- Keep up with the latest updates for your software and devices, including updates for your smartphone, computer, and any IoT devices you design or use in your business.
- Avoid sending sensitive information over public Wi-Fi, whether or not it's encrypted.
- When you do send sensitive information to a website, make sure the address starts with "HTTPS" – this will at least ensure the data you send to that one website is encrypted.

- A VPN (Virtual Private Network) app or service can give you another layer of protection for your sensitive business data. VPNs encrypt traffic between your computer and the internet – even on unsecured networks. You can get a personal VPN account from a VPN service provider. If you decide to use one, be aware some VPNs are more secure and easier to use than others, so shop around. Read reviews from several sources, including impartial experts.