Weak Security iPhone / IPad

Weak Security iPhone / IPad | Tech Tips Article by PcCG

Users who have recently upgraded to IOS 14 or later may have suddenly received a notification that their wifi security is weak. The exact message states something like:

"*Weak Security*
WPA/WPA2 (TKIP) is not considered secure.
If this is your Wi-Fi network, configure the router to use WPA2 (AES) or WPA3 security type."

Don't Panic. It's unlikely your network is being overrun by people hacking away at it, stealing your data left and right. You may have people interfering, mining, or doing other malicious things -- even just borrowing your internet, but the odds of that are slim, almost zero. That being said, it is worth while to look at upgrading your wireless security.

First lets define a little terms and spend a moment understanding the terms/technology a bit better.

The first set of letters (WEP/WPA/WPA2) refers to the certification...maybe like the "protocol" being used. This defines a broad set of rules that can be used to communicate within the certification. The second set of letters is the standard to which devices agree to communicate with - think of this as a more specific, strict set of rules. We've encountered this idea in every day web browsing.

Using the web on a day to day basis, you may have noticed some sites are HTTP (although fewer these days), and others are HTTPS (the majority of sites I'd argue). Both are following the HTTP general rules, but HTTPS has a more specific set of secure rules that fall within the HTTP subset. Going back to Wifi, you may have the WPA2 certification which runs TKIP ("Temporal Key Integrity Protocol") or AES ("Advanced Encryption Standard") standard.

Again: WEP/WPA/WPA2 are certifications (broad). TKIP and AES are standards (specific rule sets).

In most situations, I would suspect this new scary sounding warning is due to a router setting that simply ALLOWS devices to fallback to TKIP. Most routers have settings to operate at a single specific certification and standard (WPA2-AES) or often, and by default are set to "WPA2 TKIP/AES". This setting would allow for obviously TKIP or AES devices. This setting is useful for older devices that may only support TKIP, the first of the two standards supported on wireless routers. I would suspect that this is the default setting in many routers – primarily to prevent an influx of trouble calls to companies. If the routers defaulted to WPA2-AES only, user claims their router(s) are no good because whatever device can't connect to it – failing to understand that it's their device that doesn't "speak AES," the more secure standard.

Today however just about everything is capable of operating under WPA2-AES. If it isn't capable, then it may be time to consider replacing said device anyways.

For the droves people receiving the scary message that their wireless network isn't secure ; you likely need to log into it and disable the TKIP/AES option, and set it to AES only; or more specifically WPA2-AES. The million dollar question is how do you do this? While usually not too difficult, I can't possibly cover the thousands of different model makes and types out there. I can tell you in general it goes something like this:

- Log into your router (http://192.168.1.1 [1] or http://10.0.0.1 [2] or http://10.1.10.1 [3] or http://192.168.1.254 [4]). Those are the most common router login addresses. Enter your user name and password. If you don't know it, or never set it, you can try username: admin password admin; or username admin, password blank (meaning leave it empty). If those don't work, check the writing on the router, usually the back or bottom; it may contain login info. (Note the wireless key or wifi key or wifi password is NOT typically the same as the LOGIN password. Once password logs you in to make changes like we're trying to do here; the other gets you on the network to use the internet).
- Head to the "wireless" tab/section.
- Modify your Encryption type somewhere on this page. If you can't find it there, you may find it under "security" as a sub-category of the wireless page.
- Probably best to not mess with anything else if you don't know what you are doing.
- If you do feel comfortable – it may be worthwhile to back up your current configuration and then update the firmware while you're at it! (Firmware is sort of like the operating system of your device… router in this case. This of it as upgrading from Windows 7 to Windows 10.) This may provide more of a security improvement than tweaking your wireless settings.

For those that have no clue how to make this change, reach out to your local I.T. shop and schedule a time to have them make the change for you.

Protecting your wireless network is important. After all, we use wifi and send/receive so much sensitive data across it. Being paranoid; usually isn't as helpful. For most people in most situations, your network is probably already secure. It never hurts to make sure though. Assumptions….. well, we all know how those work out.

Article Tags: Tech Tips [5]

Tech Tips Articles [6]

Source URL:https://www.pccomputerguy.com/tech-tip-article-iphone-weak-wireless-not-considered-secure

Links
[1] http://192.168.1.1 [2] http://10.0.0.1 [3] http://10.1.10.1 [4] http://192.168.1.254 [5] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips [6] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Articles