Rogue Access Points

December 11th, 2015

We've all been there. It's been a long day of shopping at the mall, or waiting in an airport, or driving across the country, and we finally get a chance to pull out our phones or laptops and look for WiFi. Good news: You've found one that doesn't require a password! Free WiFi saves the day. You click accept and head to your favorite place to watch videos of kittens, or whatever people normally do on the Internet … we mostly watch kittens.

There's just one problem: what if that free WiFi was a trap? One of the cleverest phishing scams out there right now is built on the lure of free WiFi using rogue access points, and it has enough variations to stay ahead of the security teams at Apple, Samsung, Microsoft and our own security for one simple reason: The soft spot in your security is you.

Here's how phishing on rogue access points works: The scammer will set up a wireless router offering free Internet, often marked "Free WiFi," "ATT WiFi," or "Starbucks." Would you be suspicious of those networks? Many people just look for the strongest "free" network, while most of the rest of us look for a name we trust. How paranoid do you have to be to not connect to Starbucks WiFi at the mall? Once you connect, though, they have a variety of ways to get any information they want off your phone or laptop.

Even scarier, some scammers are using programs that tell your phone that the name of the free wireless available from the scammer's router is whatever name your phone is looking for, so it can even connect automatically while in your pocket. You can get phished over your phone just by walking in the wrong area.

Once you're on their network, they have a variety of ways to steal your info, from just grabbing your session cookies to using keystroke monitors to get logins and passwords, to the traditional phishing technique of creating dummy sites that look like Facebook or major credit card websites to prompt you for your info.

Here's what you can do to stay safe:

1. **Turn off your WiFi unless you're at home or work.** I know, I know. The only thing worse than mobile network data speed is mobile data network pricing. Well, maybe mobile network customer service. Unfortunately, all that WiFi you grab every day can be dangerous. Even if you're not running into rogue access points, you've still got to hope that the coffee shop or burger joint actually pays attention to the security of their wireless router, which few even think to do. Even those businesses that do think about security rarely spend money on it – rarely are they bringing in a professional. No, they're asking a minimum wage employee to "take care of it" because "you're young and good at computers." On a related note, isn't it odd that coffee shops don't spend more time thinking about their WiFi? Isn't that a core business at this point?

2. **Even then, make sure your home and work WiFi are safe.** Endpoint security, like Norton antivirus, is not as effective as it once was, simply because there are so many more points of vulnerability than there were a few years back. We'll have an extended look at securing your WiFi network in a future installment, but for today, set up your password with WPA2 Enterprise encryption. If your router does not support it, it's time for a new router.

3. **Rename your home network something like "This Public WiFi is UNSAFE."** It might sound weird, but if a scammer tries to use software to tell your phone the name of his network is the same as your home network, your phone will tell you it's connected to "This Public WiFi is UNSAFE" and you can get off of it.

4. **Apps are your friend.** Most apps, including ours, use HTTPs security, rather than HTTP. This can actually stop some of the tactics many scammers use. Remember, they don't want to beat the best security; they want to do as little work as possible and beat those unwary souls who rely on the worst security. A simple step up is enough to keep many scammers at bay.

5. **Get an app that prevents rogue access.** Depending on your operating system (OS), you have different options, but search your app store. It's worth the trouble and $4.99.

Sources:

http://www.wikihow.com/Secure-Your-Wireless-Home-Network

https://www.reddit.com/r/AskReddit/comments/3v98uz/what_are_the_best_computer_hackers_able_to_do/

http://networkengineering.stackexchange.com/questions/123/how-do-you-prevent-rogue-wireless-access-points-on-a-network

http://www.inc.com/security/articles/200801/accesspoints.html