What channel is the food network on comcast xfinity

About a year ago, Comcast began modifying the routers of some of their customers to create an almost public wireless system called XFINITY WiFi intended for use, primarily, by Comcast customers. Home users will see a new Wi-Fi network called xfinitywifi along with their existing private wireless network. In pushing the program, Comcast points out that when one of their customers visits another, the visitor can use the xfinitywifi network rather than the host wireless network. They touted it as a security feature, since homeowners are keeping their Wi-Fi passwords secret. Of course, this ignores the fact that many routers offer guest networks to solve this problem. The big benefit is that when Comcast customers are traveling to an area served by Comcast, they can use this public Wi-Fi to go online. XFINITY Wi-Fi can save 3G/4G bandwidth which is usually limited and it should also be faster.Comcast makes XFINITY WiFi available to their business customers and they have installed it in some public areas, such as Universal Orlando Resort. It could even allow someone to get away with a cheap wi-fi tablet just as opposed to a model with built-in 3G/4G/LTE. The company claims to have more than a million XFINITY WiFi hotspots, another source put the current figure at 3 million. Either way, Comcast plans to have 8 million by the end of 2014. To put this in perspective, Comcast has about 21 million Internet customers. Is Xfinity WiFi a good thing or a bad thing? In the This Week in Tech podcast on June 15, Leo Laporte didn't know what to think. At Lifehacker, Melanie Pinola recently wrote It's not necessarily a terrible thing. They, like many others who have covered this topic, probably did not consider all security issues. Here I will cover the obvious downsides to the service, some less obvious limitations, and finally, a new security risk that no one has yet raised. Focusing on defensive calculations like me, XFINITY WiFi seems like a bad idea for Comcast customers, both those who offer free Wi-Fi on their routers and those who use systems away from home. If you read this whole article to the end (warning: it's long), I'm sure you'll agree. The first reaction that many people have is the fear that outsiders connected to their home router will hog the bandwidth and slow down the internet connection speed of the host. In response, Comcast says they do not allow more than 5 xfinitywifi guest users at a time on any one router. They also say that Broadband connection to your home will not be affected by the XFINITY WiFi feature... We have provided the XFINITY WiFi feature to support strong use, and therefore, we anticipate the impact of to an indoor WiFi network. DOCSIS 3.0 cable modems get their speed, like the ac taste of using multiple channels. Unlike Wi-Fi channels, DOCSIS channels refer to wired connections between the cable modem and the cable provider's home office. Some DOCSIS 3.0 modems have 4 channels in each direction, others have 8 downstream channels (from the Internet for you) and 4 upstream (from you to the Internet). It is possible that Comcast port devices (Arris Touchstone models in Houston) are configured to send guest traffic through another channel or channel with traffic from the host. But, to be clear, this is speculation on my part. I didn't run through any tests in hard quantities, but my expectation would be that the bandwidth impact would be minimal. Another obvious problem is that visitors can interact with computers and other devices on personal networks (wired or wireless) because everything connects to the same gateway device. Addressing this issue, Comcast says the XFINITY WiFi Service is designed to work on a separate network so that your home network remains completely secure. Here too, I didn't run through any reports that put this claim to the test. Samara Lynn, of PC Magazine, raised another concern - physical security. She writes that People locate Comcast hotspots through an Xfinity app or through the Xfinity hotspot location website. I would be worried about my address being broadcast by the app or website. Comcast did not address this, but Lynn said Comcast's vague statement on the matter was not reassuring. IT WASN'T METhe last of the objections was clearly responsible. What if a guest, using an Internet connection in your home, does something illegal? Something so bad that law enforcement agencies are involved. This has come up many times before and perhaps, the most important reason not to share your home Internet connection. For the outside world, all computer devices in your home look the same. That is, they share a common public IP address (an IP address is the only number that identifies a single domain on the TCP/IP network). You can view your public IP address ipchicken.com, ip2location.com, and more. Nothing I've read says that guest XFINITY WiFi is given their own public IP address. If they don't, anyone who provides services from their home, runs the man's risk with guns knocking on their door. Comcast said that if the FBI comes knocking on doors, there's no need to worry; Illegal activity can be traced back to the customer who is a known Comcast client. Comcast has said this, however, suggests that illegal activity is not easy to trace the real culprit. And even if Comcast can involve any illegal activity for their client who is a guest on your home router at 9:56 a.m. on Tuesday, you'll trust one which companies hate most in America to have your back in this case? That there is no detailed explanation of how this works, just make a detail In addition, XFINITY WiFi is not limited to Comcast customers, making the task of identifying the real culprit of illegal activity much more difficult. As shown in the screenshot below of the Comcast FAQ page, there are two ways that anyone can jump on the system: a free trial and a short-term access card. Bad guys with stolen credit cards can get online for an hour ($2.95), a day ($7.95) or a week ($19.95). Bad guys without credit cards can use two free sessions of one hour each. To be fair, Comcast only offers one-hour free sessions at selected XFINITY WiFi hotspots. But exactly that means, they don't say. Similarly, access cards are not available in all locations. Whether that means you can't buy them everywhere or you can't use them everywhere, again, isn't spelled out. THE LESS OBVIOUS DANGERSThe first problem with Comcast claiming that the guest network is separate from private network hosts is that there are no technical details on how this is done. Data traffic needs to be segregated on air, in routers and as far as anyone on the Internet can distinguish. Comcast did not say if xfinitywifi traffic was encrypted on air, a huge omission. Their FAQ page has a related question: Whenever you sign in, we help protect your privacy and the safety of Your Comcast Email or your username and password by providing 128-bit encryption on the sign-in page. In other words, their sign-in page uses HTTPS. WPA2? It's none of our business. Heck, they don't even say which Wi-Fi band (2.4GHz or 5GHz) they use. Is this document distressed by ineficiency or is it carefully crafted to hide scrutiny in technology? However it is done, the device that separates public and private networks in your home is the port device, a combined modem and router. Next month, at the Hackers On Planet Earth (HOPE) conference, I will give a presentation on Security a Router Home. In part, I was attracted to this topic because of the massive parade of terrible security vulnerabilities in the routers. It seems that when it comes to router firmware, quality is the work of 326.With 8 million of them in the field, the devices used for XFINITY WiFi will definitely be the main target for bad guys. If they make mistakes, someone will definitely find them. A security issue related to userid/password is used to log on to XFINITY WiFi. It is the same used to log into the Comcast website to manage an account. If a bad guy has kept it (more on this below) there is a huge potential for abuse. They can view your payment details and read your web email. They can add HBO and to your account. Worst of all, they can log into XFINITY WiFi like you, do something illegal and have everything point back to you. A much better approach would have been for Comcast to let their customers create a new userid and password, one that is only valid for giving Wi-Fi. Better still, there should be a Wi-Fi-only userid/password for each family member. A single userid/password being used for everything is too attractive a goal. MAC ADDRESS SPOOFINGPerhaps the biggest security issue with XFINITY WiFi related to Auto Login. According to Comcast anyone who uses XFINITY WiFi when away from home only has to log in with their Comcast userid/password once from any certain wireless device. Then, the system recognizes the device automatically. ... once you have successfully logged in using a Wi-Fi-powered device, your device will be registered automatically login and you will not be asked to provide your Comcast ID and password to connect to the XFINITY WiFi network using the same device... You can sign up for up to 20 Wi-Fi-powered devices using our automatic sign-in feature. After the previous point, this seems like a good thing, since using Comcast / password is not sent through the air. I suspect, however, that it is a major security flaw. How do I do this? No need to say at this point, I can find no relevant documents. How can it work? If Comcast requires their software on wireless devices, then their software may generate certain types of unique identity codes known only to Comcast. But their software is not necessary. Any device that supports wireless can log on to XFINITY WiFi. So how can Comcast uniquely identify a particular device? By MAC address (MAC, all of the above cases, is a network identity; Mac, with ac in the lower case, is a computer from Apple). All wired and wireless network hardware has a unique 48-bit identity called a MAC address. From the very beginning, MAC addresses were uniquely designed globally. The first 24 bits identified the company that created the hardware, the last 24 bits acted as several series for the device. A router has at least three MAC addresses, one for its WAN connection to the Internet, one for its LAN connection and one for its Wi-Fi radio. A dual band router will have a MAC address for each wireless band. You can usually find the router's MAC address on the sticker at the bottom. If you've ever handled a router configuration, you may have run through a security feature called MAC address filtering. This lets you tell your router the MAC addresses of known trusted Wi-Fi devices. These devices are allowed in, all other devices are blocked. You can see a demo of the MAC address filter configuration for an Asus router here. Sounds like a great security feature? No one uses it. In fact, it offers virtually no security, at least for wireless. Mac addresses are always broadcast uncoded through the air. Basic communication protocols required This. So anyone who finds themselves blocked by a router using MAC address filtering, can only listen to a valid MAC address that communicates with the target network and then pretend to be Device. Pretending (called a forgery) is not all that difficult. Back in XFINITY Wifi, we can now understand what I see as its biggest security problem. Instead of using a free session for an hour, a bad guy can park near an xfinitywifi network and make a note of the MAC addresses of devices that use the network. Then all they need to do is fake their MAC address, get automatic login, do something illegal, and an innocent Comcast customer is in for all sorts of hell. There's no defense here, too. The best security for public Wi-Fi networks, VPNs, does not protect prevent bad guys from seeing your wireless device's MAC address. A VPN encrypts content, but it's sent to the router in a series of bits (the package is the official term) including an unedicrypted MAC address. That said, Comcast has been launching XFINITY WiFi for the whole year. At the very least, they have more than a million hotspots. It's hard to believe I'm the first to publicly raise this issue. So I did some searching, and found a six-month-old reddit post where someone claimed that spoofing their MAC address to aa: bb: cc: dd: ee: ff (all valid hexadecimal digits) got them on a CableWiFi network without having to provide login information. If true, it would not be a surprise. It also means (if it is true) that the CableWiFi system keyed off the MAC address. And if they do, it's likely that XFINITY WiFi does too. EVIL TWIN NETWORKSAfter, there are classic Wi-Fi problems - evil twin networks. Last June, when Comcast was offered free access to their Xfinity WiFi system for the July 4 holiday, I was warned about the evil twin network. My main point is to assume a wireless network called xfinitywifi actually belongs to Comcast is a leap of faith. Page 2 That anyone can name their network anything, is probably the biggest skeleton in the closet for Wi-Fi. Comcast customers have no way of knowing that they are actually communicating with a Comcast router when they log on to a wireless network called xfinitywifi and provide comcast userid and their password. This was also the case at Starbucks, Barnes and Noble, airports, etc. A few days ago Sean Gallagher at Ars Technica wrote about his experimentation on an evil twin network for attwifi. This is very common, that Hack5 offers a pineapple WiFi device for just the kind of thing. Greg Foss went so far as to create the necessary html and scripts to mimic an XFINITY WiFi login page. He calls it pineapple Xfinity.And, that's just the original XFINITY WiFi login. What about all the other times can someone use an xfinitywifi network? Comcast automatically logs in to devices it has seen before, making these sessions also dangerous. As a rule, automatically reconnect to the Wi-Fi network they saw before. That's cute. How ridiculous, considering the definition of a one they have seen before what is nothing more than easily faked network names (also known as SSIDs). If my wife is a wireless device, she will go home to anyone named Michael Horowitz, and there are quite a few of us. So customers who have joined an xfinitywifi network, potentially having their wireless device join another one, be it from Comcast or not. Smartphones and tablets are online devices. Although there may be no display indicateds, apps that run continuously in the background send and receive data over the Internet. These un encrypted apps will leak a treasure trove of information to a bad guy who runs an evil twin network. Someone I know was recently surprised when their Android device informed them that they have a Time Warner cable bill due soon. The My TWC app called home to find out this. Is the conversation between the app and Time Warner encrypted? Who knows? An iPhone may have chosen to make an iCloud backup while it is connected to a fraudulent xfinitiywifi network. Without a friend who is fluent in sniffing packages, there is no way for smartphone owners to know which apps encrypt data in transitions. Even data encryption apps can leak personal information like NPR discovered when Steve Henn recently partnered with Sean Gallagher of Ars Technica and Dave Porcello of Pwnie Express. Their packets have discovered security vulnerabilities in some services. And that's just when a fraudulent Wi-Fi network is passively listening. If the bad guy behind it wants to, he can carry the man in the middle attacks that make almost all the security arguments online. Again, this is an inherent problem with Wi-Fi, it is not specific to XFINITY. Over at Ars Technica, Sean Gallagher points out that AT&T is T configure their smartphone to automatically connect to attwifi hotspots out of the box. He added The same tools I use to forge Xfinity can be set up to automatically answer a victim's phone like any Wi-Fi hotspot they already trust. That's because of the exploration requests generated by your smartphone and Wi-Fi — when you turn on your phone's Wi-Fi connector, it searches for any network you've ever connected that it wasn't asked to forget. If Comcast requires customers to log on to XFINITY WiFi each time, then automatically connecting to the evil double network will not be a security issue, on the legitimate xfinitywifi network. Any device connected to the router / port will not be allowed immediately to the internet. Convenience has always been an enemy of security. Update: BTWiFi in the UK is very similar to XFINITY WiFi. It requires the user to log in at all times. But this restriction will not apply to evil twin xfinitywifi networks. Bad guys will be willing to allow you online without a password to them can track your activity. But, even this effort conveniently causes problems. Three of the questions on the Xfinity Xfinity FAQ page agreement the device is too eager to connect to XFINITY WiFi. My device is always connected to xfinitywifi signal - how can I set my own home network as the default? I can't connect to my own Wi-Fi network or printer. What's wrong? Even when I'm at home, my device is always connected to xfinitywifi signal - how can I set my own home network as the default? Ars' Gallagher found his iPhone automatically connected to a neighbor's xfinitywifi network. After using an XFINITY WiFi network or any common network like attwifi, the safe thing to do is to prevent your wireless device from automatically connecting to the next network with the same name. This is harder than it should be. As far as I know, both iOS 7 and Android 4.x cannot prevent automatic reconnection to previously used Wi-Fi networks. Having an option in iOS 7.1.1 (Settings -&gt; Wi-Fi -&gt; Network participation requirements) sounds that way, but it only applies to new networks. Apple is very clear that known networks will be joined automatically. One exception appears to be Android phones from AT&amp;T T, where you can disable Automatic connection to AT&amp;Wi-Fi hotspots; T when detected. So that means we have to convert attwifi, xfinitywifi, CableWifi and other popular network names from known unknown states. On Android, this is easy. At the bottom of the list of Wi-Fi networks detected are networks that are not currently in range. Long press on a network to reveal the option to forget it (ion to make it unknown). On iOS this is not easy. In my test, iPads running iOS 7.1.1 don't show previously used networks that are currently 100% 100% earlier. Maybe there are some, maybe none. And the networks currently being discovered can only be involved, not forgotten. The only way to forget a personal network seems to be to connect to it for the first time. Only then does the option to forget the network appears. There is, however, a big hammer - delete all network settings. In iOS 7.1.1, perform Settings -&gt; -&gt; Reset -&gt;Reset. Then again, Apple users using the iCloud Key sequence can also find Wi-Fi networks from their laptops re-populating their iOS devices. And since iOS 7.1.1. does not reveal the list of known networks, this can easily go 900% 100% 100% away. Ugh. Personally, I leave the house with Wi-Fi disabled. Wi-Fi performance Although security is much more important than performance, we can expect XFINITY WiFi to cause wireless slowdown. Comcast can allocate more wired bandwidth between your home modem/router and themselves, but they can't allocate more Wi-Fi channels. Within 2.4GHz, things can get ugly with extra guest users. In crowded areas, the frequency range was overloaded and not only with Wi-Fi users (my microwave interference with my Wi-Fi something terrible). If the xfinitywifi network runs on the same channels like home networks, which will inevitably lose bandwidth for private Wi-Fi users. If the xfinitywifi network runs on a nearby channel, things could be even worse as most available 2.4GHz channels overlap. For example, a network on Channel 7 appears as strong radio interference into the network on Channel 6 and vice versa. Everyone suffers. Both networks would be better on the same channel where they could use the traffic police feature of the basic protocol to avoid trampling on each other. Sebastian Anthony of ExtremeTech recently wrote that overlapping channels are the main reason for terrible through throughotechnies on your wireless network. The only non-duplicate 2.4GHz channels are 1, 6, and 11. The best case for private home users with networks running on Channel 6, for example, is for xfinitywifi networks that use channels 1 or 11. But, that will create interference for anyone in the region using those channels. There are no good options in the 2.4GHz band. So how does Xfinity WiFi allocate channels? Peter Lewis asked, but he got nowhere.Comcast doesn't come clean about this, saying that wifi networks in your home, as well as XFINITY WiFi, use universal sharing, and as with any shared media can have some impact as many WiFi sharing devices. TRUST COMCAST With a lot of unknown specifications (a full list is below), the use of XFINITY WiFi system requires trust in Comcast. Is this a reasonable thing to do considering how many of their customers hate them? (see more here) In this study I read my share of XFINITY WiFi documentation at Comcast.com. Many times they provide links where customers can sign in to their accounts to make changes. The link is to , a page where customers enter Comcast userid and their password. No one should enter a password on an unsafe HTTP site. That's what HTTPS is for*. And Comcast has a secure HTTPS version of the page. They just don't bother linking to it. Then, too, consider that XFINITY WiFi is being activated by default, customers must actively opt out. TURN IT OFF Comcast has said that only 1% of their customers have chosen to disable XFINITY WiFi. It may not be the egregious exclusive overreach that Sebastian Anthony calls it, but my guess is that most Comcast customers don't fully understand the risks. If you know a Comcast client, you'll make them a priority to point them to this blog. There are three ways to disable XFINITY WiFi.1) go your home network. Sign in, then click Users &amp; Interests, then Manage XFINITY Wifi. There have been, however, many reports of site errors with this.2) Call 1-800-XFINITY3) Don't rent a box (Comcast calls them ports) from Comcast. Instead, buy your own cable modem and your own. A commenter below indicates that with services from Comcast, buying your own modem is not an option. In this case, have Comcast modify their port so that it runs in bridge mode and then add your own router. (Updated July 2, 2014) THE OUTSTANDING QUESTIONComcast is not my ISP, so there are so many aspects of Xfinity WiFi that I can't check or verify. This is what I don't know. Do guests and hosts share a public IP address? Otherwise, do all guests share the same public IP address? How are Wi-Fi guests separate from private networks? Vlan? Different IP child networks? When the FBI comes calling, how does Comcast distinguish traffic from a guest user versus host? Can Comcast distinguish traffic between different guest users? Is automatic login to XFINITY WiFi keyed off MAC address? Does XFINITY WiFi work at 2.4GHz band, 5GHz band, or both? In the 2.4GHz band, how does it allocate a Wi-Fi channel to the xfinitywifi network? Same question in 5GHz band Is there any air encryption like WPA2-AES? Update January 3, 2015: The xfinitywifi networks I've seen since writing this article are uns secure. No WEP, no WPA, no WPA2. Does turning on XFINITY WiFi slow down your private network? If a customer chooses not to join XFINITY WiFi at home, can they still use it away from home? If customers have their own modems and routers, can they use XFINITY WiFi when away from home? According to a comment below, the answer is yes. Can non-Comcast customers, with a free trial or short-term access card, access the home router? How fast is guest connection? If I learn more, I'll update this blog. *In the unsafe HTTP version of customer.comcast.com, the IFRAME password entry form is included in the page with HTTPS. However, because IFRAME is transmitted inside an unsafe page, it can be modified during shipping before you see it. So userid and your password can be sent to the bad guys. One of the benefits of HTTPS is that it ensures data is sent as the data received. NOTE: As mentioned above, I will be talking about Protecting a Home Router at the HOPE (Hackers on Planet Earth) conference next month. The conference took place in New York City from July 18 to 20. My presentation was on December 20 at 3:00----------------------------February 11, 2015: The San Francisco Chronicle reported on December 9, 2014 that Comcast was being sued for turning home Wi-Fi routers into public access points. Copyright © 2014 IDG Communications, Inc. Inc.