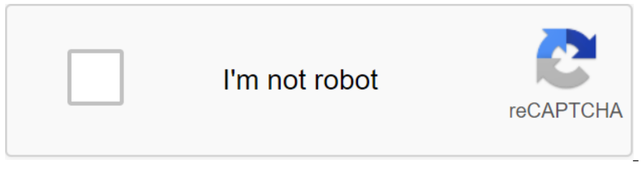
Vodafone wifi router manual



Continue

Photo: D-LinkTech 911Tech 911Do Do you have a technical question to keep you up at night? We would like to answer it! The electronic david.murphy@lifehacker.com with Tech 911 in the subject line. In this week's technology tips column from Lifehacker, we're going back to our favorite topic: wireless networks. This time, the reader has some issues getting an important piece of old gear to work with an important piece of new gear. If you've ever upgraded a router, or plan, this situation should be all too familiar. Lifehacker reader Ashley writes: I came across one of your articles about safari and can use some tips. So my aunt and I live on the same property, 200 feet apart. She had Wi-Fi for the past year and my extender always picked up the signal without problems. Up until a week ago when it got a new router. So my question is, how can I restore my extender? I would do it myself, with some instructions if possible. Thank you in advance! Every week, Lifehacker's senior technical editor answers your toughest technological questions.... More I'm going to start with the good news: This problem should be easy to fix, except for any unforeseen circumstances. For starters, I'm going to assume that your new Wi-Fi router is pretty decent, and you have no problem getting a signal from where you created the wireless extension cord. The quickest way for your extender to jump back to your wi-fi router connection is to ask your aunt to use the exact same SSID and password on her new router that she used on her old router. The extender knows nothing better; it should connect to a wireless network without any problems at all. However, there is one small caveat that can screw up the process. If you previously set up an extension to connect to the 2.4GHz router network, and your aunt, for whatever reason, only using 5 GHz on her router, this pairing won't work. (A more likely scenario for your aunt would be to use only 2.4 GHz on her router, and you have previously installed an extension to connect to the router of the currently defunct 5GHz network.) How to access typical Netgear extension cord settings. Screenshot: David MurphyYou can always pull up wireless extender settings to make any changes needed to make the connection work again - connecting to the new SSID if your aunt renamed the Wi-Fi network, or setting up a wireless band that your extender uses to connect to the router. I recommend working web searches for your model extension cord numbers and pulling up your manufacturer's instructions since that you enter into your web browser to access its settings may be different. (As a bit out of the way, I recommend not using your dual-connection extension option if it has one or something similar to the name. For better performance, just connect the extendator to the router 2.4 GHz or or or Network. When you create a second Wi-Fi network that shoots from your extender, isolate it to the opposite lane if applicable. So if you connect to a 5GHz router, your devices should only connect to the 2.4GHz expansion frequency, for example.) If you're a little confused by the screen of the main puller settings, or you just don't want to fuss with it, try the nuclear approach: Factory-reset your extension cord. Normally, you can do this by holding the reset button, assuming that it has one, for 5-10 seconds, until the lights on the extension cord start flashing differently. To make sure you are doing this process correctly, however, check your device's guide. Once you've done this, you can follow your manufacturer's initial installation instructions for your extender, which should make it easy to connect it to your aunt's new router- you got your extension running properly for the first time, after all. If you're still having trouble connecting, try moving the extender a little closer to your aunt's router (or move it to the router a little closer to the extender) and see if it helps. And make sure you've updated your extender and router for your latest firmware versions. You should be able to check which firmware your router and extension cords are used in each device's web screen settings. You can then check the device manufacturer's support site to see if the latest firmware it offers is what your device uses. If not, update it! And if it still doesn't fix the problem, there are many other reasons why you may have difficulty communicating, and we've covered them in detail: Let me know if this advice helps. If not, I'm happy to keep troubleshooting! Do you have a technical question to keep you up at night? Tired of troubleshooting in Windows or Mac? Looking for tips on apps, browser extensions, or utilities for a specific task? Let us know! Tell us in the comments below or email david.murphy@lifehacker.com.Page 2Screenshot: David Murphy (YouTube)Tech 911Tech 911Do do you have a technical question to keep you up at night? We would like to answer it! The electronic david.murphy@lifehacker.com with Tech 911 in the subject line. We're solving a funny problem with a calling-me-down at Tech 911 this week. I wish I knew someone older than me- a parent, a brother, an amazing neighbor who has laptops and smartphones and gadgets galore that they can go my way when they are tired of using them. Unfortunately, I don't know, but Lifehacker reader Kyle certainly does. And while free things are always fun and appreciated, there is one quirk with his latest that he needs help addressing. He writes: I was given an old mac (cheese grater one) and I have no entrance. What can I do to use the machine? For the purposes of this answer, at least the first part of it-I'm going to suggest, suggest You ask how to enter the car if you don't have a username and password. This question speaks to a broader point, however: How can I access a car that someone else has blocked? Fortunately, we don't need to worry about any crazy tools to recover or crack password tips for this, since your ultimate goal is not to get into an account that is not yours, but to use the system on which this account was previously created. In other words, we can simply reset your cheese grater by factory default and customize it as if it were a completely new system, eliminating this login problem. The easiest way to do this is by assuming that the previous owner of your Mac hasn't created a firmware password, which makes things a lot harder, is to just load into your Mac recovery mode when you run it. Power on your computer and immediately start holding Command'R. Keep doing this until you see something happen on the screen (usually an Apple logo or a rotating globe), then you can release the keys. If you don't see a macOS utility box when restoring boots, and instead see something like macOS Recovery with a request asking you to enter a user password, click on the recovery assistant and select Erase Mac. Click on the blue Erase Mac hyperlink and let the 'er rip'it will destroy your system and allow you to customize the new version of macOS from scratch (with any username). Otherwise, if you make it into the main macOS utility box, run the drive utility. select the disk on which macOS is installed and select Erase. After that, get out of the utility drive and start the process of reinstalling macOS through a handy link to the main macOS Utility screen. I hope the person who gave you your new iCloud Disabled Mac (and Find my... feature) before coughing it up. Otherwise, you should be able to reset the NVRAM of your Mac/PRAM, which removes Find My Association. Then you can log into your iCloud account and you should be able to customize your Mac as if it were always yours. (You can also simply log into iCloud as usual without resetting THE NVRAM/PRAM to link the erased Mac to your own iCloud account. This should get you up and running with your new Mac. If not, or if you are still experiencing any problems or confusion, email back! Do you have a technical question to keep you up at night? Tired of troubleshooting in Windows or Mac? Looking for tips on apps, browser extensions, or utilities for a specific task? Let us know! Tell us in the comments below or email david.murphy@lifehacker.com. Photo: Linksys While more router manufacturers are making routers easier and customize-even through convenient little apps instead of annoying web interfaces-most people people Don't set up many options after buying a new router. They log on, change the name and passwords for their Wi-Fi networks, and call it a day. While this gets you up and running with (hopefully) a fast wireless connection, and the chances are decent that your neighbor or some random evil internet person isn't trying to hack into your router, there's still a lot more you can do to improve the security of your router (and home network). Before we get to our tips, one quick caveat: Wireless routers all have different interfaces, different ways they call their settings, and different settings that you can customize. For this article, I'll be poking around the TP-Link Archer C7 interface. You'll want to explore around the web screen router configuration (or app) to make sure you've adjusted all the correct settings, but it's possible you won't be able to do everything we detail below. Access to router settingsIf your router doesn't have an easy-to-use app to customize its settings, like what you usually encounter when buying a grid network system, you'll probably gain access to its settings by pulling up a web browser (on a device that's connected to the router) and typing into the router's IP address: On the Windows system, pull up the command promptly and enter the ip address. An IP address that is listed as the default gateway is most likely your router's IP address. If you're on a Mac, pull up the system preferences of the network, and click on Advanced in the bottom right corner. Click on the TCP/IP option at the top of the next window and look for your router's IP address. If you're on your iPhone, click on the settings, then Wi-Fi, and click on the i icon next to the Wi-Fi network you're connected to. Step One: Update firmware Some routers bury firmware updates deep in their settings menu; some of them may even notify you of a new firmware update when you log in to their apps or user web interfaces. However you will find the option you are going to want to make sure that your router is running the latest firmware. If you're lucky, your router will be able to download new firmware updates directly from your manufacturer. You may have to press the button (or two) to start this process, or it can happen to auto-routers that make the latter great, because most people don't really think about checking to see if my favorite tech gear has updated the firmware on a regular basis if ever. Screenshot: David MurphyIt is also possible that your router will require you to download the new firmware yourself. If so, you Download the correct firmware from the router manufacturer, probably on the router support page, and manually update the router by reviewing this firmware file and start the upgrade process You'll have to do this every time you want to update your router with a new firmware, which means you'll have to check on the new firmware quite regularly, perhaps several times a year. It's a time-consuming process that's easy to forget, but it's also important if you want to keep your router protected from external threats. Change your login and router passwordIf you're still using an administrator/administrator, administrator/password, or any common word option to log in to the router, change that. Even if your router maker has given you a quirkier password that is presumably different for everyone, it is important to use a login and password that is hard to guess or brute force. Screenshot: David MurphyEven, if you are stuck using an admin as a username to log in, make your password something complicated, not something that someone can look through a quick search on the internet. Use WPA2 to ensure wireless network securityIt almost goes, of course, but don't use WEP when you set up a password for your Wi-Fi network. Passwords protected by WEP encryption are much easier to attack brute force than those encrypted with WPA2. Even if you're probably not someone hanging on your street corner, wardriving everyone's wireless networks, there's no reason not to use a strong WPA2 protocol unless you have an old device that just can't handle WPA2, which is unlikely. And no matter what you do, don't run an open (without password) Wi-Fi network. My god. Screenshot: David MurphyTurn from WPSOn Paper, WPS-or Wi-Fi-protected installation-sounds great. Instead of entering a long, rather complex Wi-Fi password on your device, you can simply enter a smaller PIN, probably printed directly on the router. Guess what? These PINs are much easier to rough attack than a more complex password or password. While a number of routers will time out the attacker after they fail a certain number of password attempts, that hasn't stopped the more ingenious WPS attacks from popping up. The easiest way to prevent this kind of shenanigans is to simply disable WPS completely. Yes, you'll have to enter your password. Yes, it will be annoying. It's an extra minute of your life. Everything's going to be all right. Or, if you really can't handle this process, check if your router allows you to use the WPS button instead of a WPS-based PIN. So you have to physically press the buttons on the router and any devices that you want to connect, which will make it a lot harder for someone to use WPS and break into your network. Use the best DNSBrowse on the Internet a little faster by disconnecting from your ISP's DNS and using a service like Google DNS, Cloudflare, Opendns. As an added bonus, you will also increase the likelihood that you actually make it to the websites that you are trying to visit without any person in the middle of an attack, attack, redirects, interstitials, or annoying you made a typo in your web address, so we're going to redirect you to a web page filled with spam and ads that your ISP can use. If you want to get really crafty, you can opt out of a service like OpenDNS on your child's laptop, allow parental controls to keep them out of time sucking websites like Tumblr and Reddit, and give yourself another DNS provider (like Google DNS) to browse the web without any restrictions. Your child will hate you, but at least they turn out to be a rocket scientist with 27 inventions instead of Twitch streamers with 3 followers. Screenshot: David MurphyConsider using MAC filtering, annoying as it can get Although it is easy for an attacker to fake a MAC address, you can at least give yourself a little extra security by installing a router to allow only devices to connect that appear in the white list. This filtering is based on the MAC address of each device, a long line of letters and numbers that looks like 00-11-22-33-44-55. Screenshot: David Murphy While this means you will need to go and add any new devices that you buy when you want them to be able to connect to the router, it also means that devices that you don't authorize won't be able to do squats. As I said, however, MAC addresses are easy to fake, so if this tip becomes more annoying than practical, feel free to disable MAC filtering. You'll be fine. Consider scheduling Wi-FiIf you're running a fairly normal schedule during the week, and you have no reason to remotely connect to your home devices, consider using a router planning mechanism if it has one to just turn off Wi-Fi when you're not home. This is not the most practical advice if you have a bunch of smarthome devices that need the internet as if you want to be able to turn on and off the lights to urinate from your cat or you want to be able to watch the delivery driver drop off the expensive package you ordered. If you live a relatively simple life- no harm there- and nothing really needs an internet connection when you're not around, why power your Wi-Fi for no reason? It's hard to crack a network that doesn't exist. Turn off potentially sketchy servicesY probably don't need to tinker with router settings when you're not actively connected to the wireless network. If your router has some sort of option for remote control or remote administration, make sure it's disabled. Screenshot: David MurphyYou should also consider disabling UPnP on the router, although this may you're a little heartbroken when you're playing or running BitTorrent- to name two examples. However, when the entire website is dedicated to different ways you can use UPnP for nefarious purposes... maybe it's time to go back to manual rewinding ports if necessary. Some routers also allow you to customize server, so you can transfer files to and from your network. However, we live in an age where it is easy to use any number of cloud storage providers or file-sharing services. You probably don't need to run FTP at home, and it's much safer to disable this feature completely (if your router supports it). You also probably don't need to access the router via SSH or Telnet-off either off if it's offered, and you probably don't need to access any USB-connected printers or storage when you're not home. In short, if the router allows you to do something from afar, consider turning off the function (if you can). The fewer ways you access your home network when you're not in it, the harder it will be for someone else to take advantage of the vulnerability and gain access to your router (or your home network). If you can, consider disabling the router's cloud functionality. While it may be useful to edit router settings by logging into the manufacturer's cloud service, this is just another open door that an attacker can use to compromise a router (or network). Although you don't have a choice with some routers, usually mesh routers are always better, and safer to log into the router's web interface manually with a device that is connected to your home network, even if it's much less convenient. Consider the separate Wi-Fi network for guests and smart home devices that I've been playing, testing, and browsing routers for over a decade, and I've yet to meet someone who uses the router's guest network feature. Heck, I don't think I've ever even connected to a friend's guest network in their home or apartment. However, the premise of the guest network is great, security-wise: Your router automatically installs a second SSID for friends to use, and any device connected to it is detached from other devices in your main network, either connected to the router directly or connected wirelessly. (Most routers allow you to customize whether you want guests to see everything, each other, or anything if you need to adjust the settings a bit.) The guest network comes with an added bonus, too; You can use it for all your less secure smart home devices. If someone exploits a vulnerability in your smart light and breaks into your network, there will still be a layer of protection between your hacked device and desktop, smartphone and laptop to name a few examples. While you can also get crazy and segment from your network with individual SSIDs and VLANs, if your router supports it, it's easier which won't give you a weekend headache (unless you know what you're doing). do). do). vodafone mobile wifi router manual. vodafone b3500 4g wifi router manual