

Turn Your Home PC into a VPN Server

YOU'LL NEED THIS

TWO PCS

One PC should be a laptop.

LOGMEIN HAMACHI

Download it from www.vpn.net.

PRIVOXY

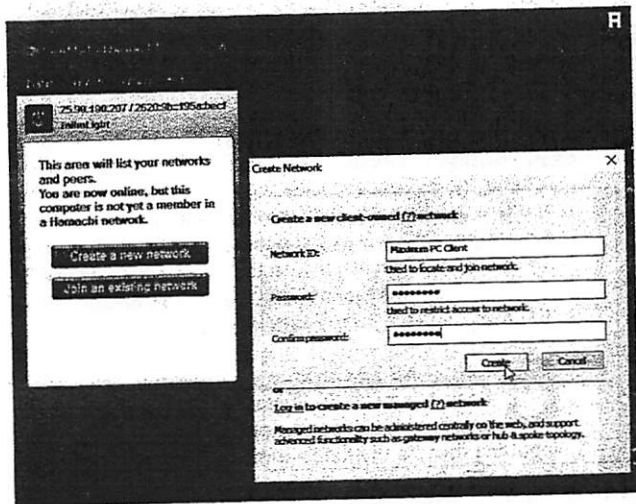
Grab it from www.silvester.org.uk/privoxy/Windows.

IF YOU TRAVEL FREQUENTLY—for work or fun—you've probably found yourself in a hotel room or a café with a Wi-Fi password scribbled on a sheet of notepaper and no idea how secure the connection is. Sometimes, you might be able to tether your laptop to your phone, but most plans don't let you make wireless hotspots unless you pay an extra fee, and it's very easy to chew through a whole month's data allowance as Windows decides it's a good time to perform some critical updates.

You can get around this problem by using a PC at home as a proxy server. Rather than data traveling directly from your laptop to the web server, it's sent via a secure encrypted connection to your home PC, which then forwards it.

This technique is only for avoiding eavesdropping on potentially unsecured public networks—it won't hide anything from your ISP. It's also worth noting that your Internet connection speed will be slower than it would be at home—particularly if you're a long way from home when you log on.

We're using a free VPN tool called Hamachi, which is mainly used by gamers to create virtual local networks, and non-caching web proxy Privoxy. Here's how to set it up. —CATHERINE EMMA ELLIS



1 PREPARE THE SERVER

This guide requires two PCs: one (a desktop or laptop) to act as the server, and a laptop, which will be the client you're carrying on the road. The server PC must be powered on at all times—something to bear in mind if you're traveling for several days.

» Using the server PC, download LogMeIn Hamachi from www.vpn.net, and run the software installer. When the program starts for the first time, click the power button to activate it, and you're prompted to create a user account, which is used to manage all your virtual networks and their users [Image A]. Do so, then verify it using the link that's emailed to you and re-entering your password. Click "Create a new network," and enter a name and password. The name can be anything you like—Hamachi identifies you using your account and device ID, so this is just for your reference.

2 START SETTING UP THE CLIENT

Now install Hamachi on your laptop, and log in using your account details. You're sent an email notification each time you log in from a new device as a security measure, but you don't need to authorize the connection. Select "Join an existing network," enter the network name and password you created earlier, and click "Join." The name of your desktop PC appears. Right-click

it and select "Browse," then enter your usual Windows account login details, and you'll see that you can access the desktop PC's filesystem [Image B].

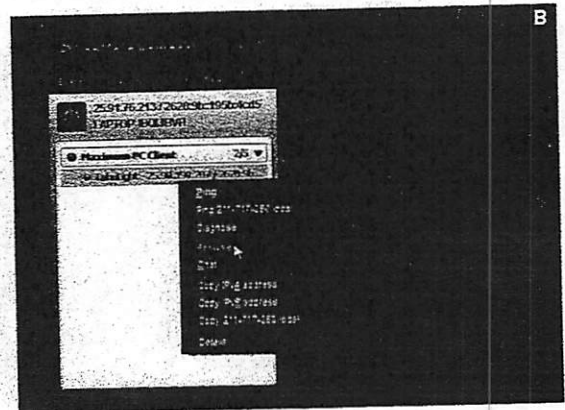
» If you have trouble connecting to the network, you might need to take a look at Windows' firewall settings, and make an exception for Hamachi. Right-clicking the client PC's name in Hamachi gives you the option of diagnosing network problems, but it doesn't offer any guidance.

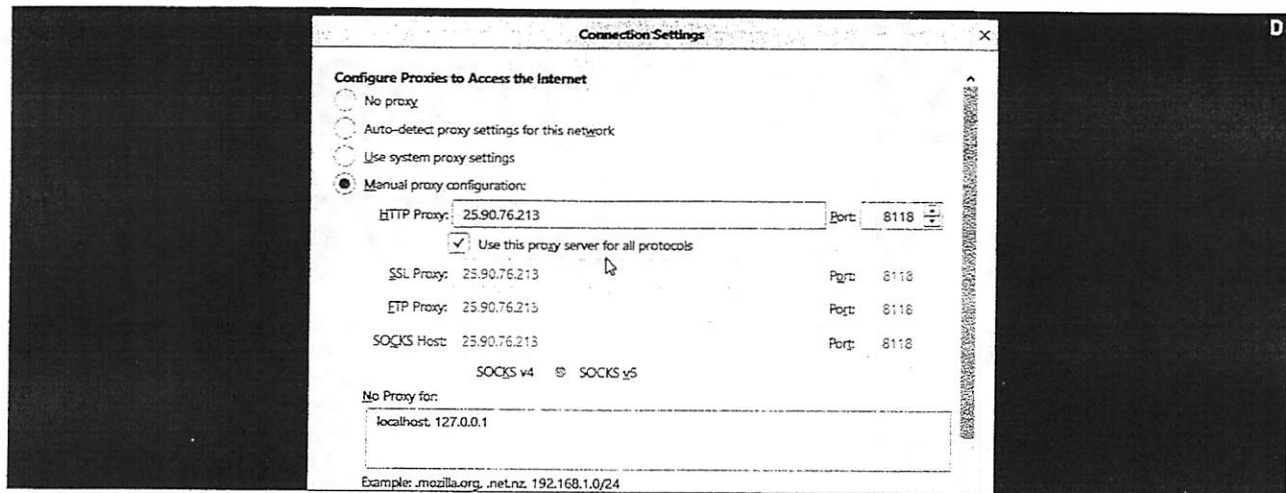
3 CONFIGURE PRIVOXY

Now return to your client PC and download Privoxy from www.silvester.org.uk/privoxy/Windows—the latest stable version of the Windows installer is `privoxy_setup_3_0_23.exe`. Run the installer, then close the empty window that appears. Privoxy doesn't have a GUI like Hamachi, so right-click the new Privoxy icon in your system tray, and select "Edit → Main configuration" to open the main settings file [Image C].

» Scroll down the text document to section 4.1, and find the line `listen-address 127.0.0.1:8118`. Type a # in front of this line to mark it as a comment, then underneath it type: `listen-address [the IP address at the top of your Hamachi window]:8118`

» Save and close the file. Restart Privoxy. The Windows firewall might prompt you to allow or deny the connection.



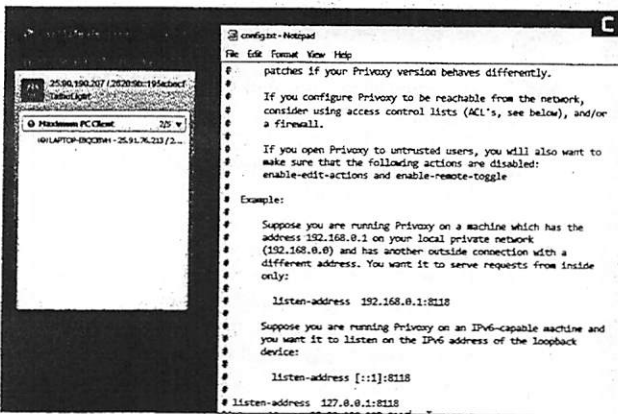


4 SET UP YOUR BROWSER Now you just need to configure your laptop browser's proxy settings to redirect network traffic via Hamachi. In our example, we're using Firefox—open the "Settings" menu, then select "Advanced," click "Connection settings," scroll down to the section on proxies, and use the network address that you entered in the Privoxy configuration file, along with the port number 8118 [Image D].

» The process is very similar for most web browsers, though Edge and Internet Explorer use Windows' own networking settings, so all network traffic is routed through the proxy—not just browsing traffic. You might prefer to limit it to your browser, to avoid system updates being downloaded over a slow connection. Browser extensions such as Foxy Proxy (<https://addons.mozilla.org/nn-no/>

[foxyproxy-standard/](https://addons.mozilla.org/nn-no/foxyproxy-standard/)) make it easy to switch between proxies, and are also worth considering for their added convenience.

» Once it's configured, visit www.privoxy.org/config, and you should see a message informing you that Privoxy is enabled. If so, congratulations—you can now take your laptop away, and connect to the Internet securely via your server PC. If you don't see such a message, the issue is likely to be your firewall settings, or a conflict with an existing proxy that you've forgotten to deactivate.



5 PRIVOX SECURITY OPTIONS

Privoxy's default settings are fine for getting a secure connection up and running quickly, but the software is also highly customizable. Right-click its icon in the notification panel on your server PC, and select "Edit → User Actions" to tailor its options to suit your Internet use. For example, Privoxy doesn't cache cookies by default, but you can choose to override this for certain sites you visit frequently to avoid having to log in each time. You can also choose whether to exempt some sites from Privoxy's built-in ad-blocking, and filter out annoying page elements. The comments in the file are quite self-explanatory, and you can find detailed instructions at www.privoxy.org/user-manual/actions-file.html.

» To be safe, it's a good idea to make a backup of any configuration files before you change them, so you can easily restore them if any of your changes prevent Privoxy from loading, or stop certain pages working, and you're not sure how to reverse the change. ☺

OTHER SECURITY OPTIONS

Setting up your own proxy server isn't the only way to secure your browsing when you're away from home. Another option is to use a VPN service, which does the hard work of encrypting the data and redirecting it for you. You can usually choose from a list of servers in locations around the world, which makes it a good way to avoid region-blocking.

There are some free VPNs around, but all of them have strict data transfer caps

that make them impractical for anything more than checking a few emails; 100-500MB per day is the standard offering. If you travel frequently, it's worth considering a premium VPN service such as Hotspot Shield Elite, AnchorFree, or TorGuard. This is the only viable option if you want to download large files or stream video over a secure connection, but it's wise to research your options carefully beforehand—some VPNs log

more of their users' activity than others, and for different periods of time.

Another option is Tor Browser, which re-routes browser traffic through a network of nodes around the world, not just one server. Its main disadvantage is its slower speed. The data is decrypted at the last node, so there's a small chance that it could be intercepted at this point, but it's otherwise one of the best ways to keep your browsing private and secure.