

Internet Connections



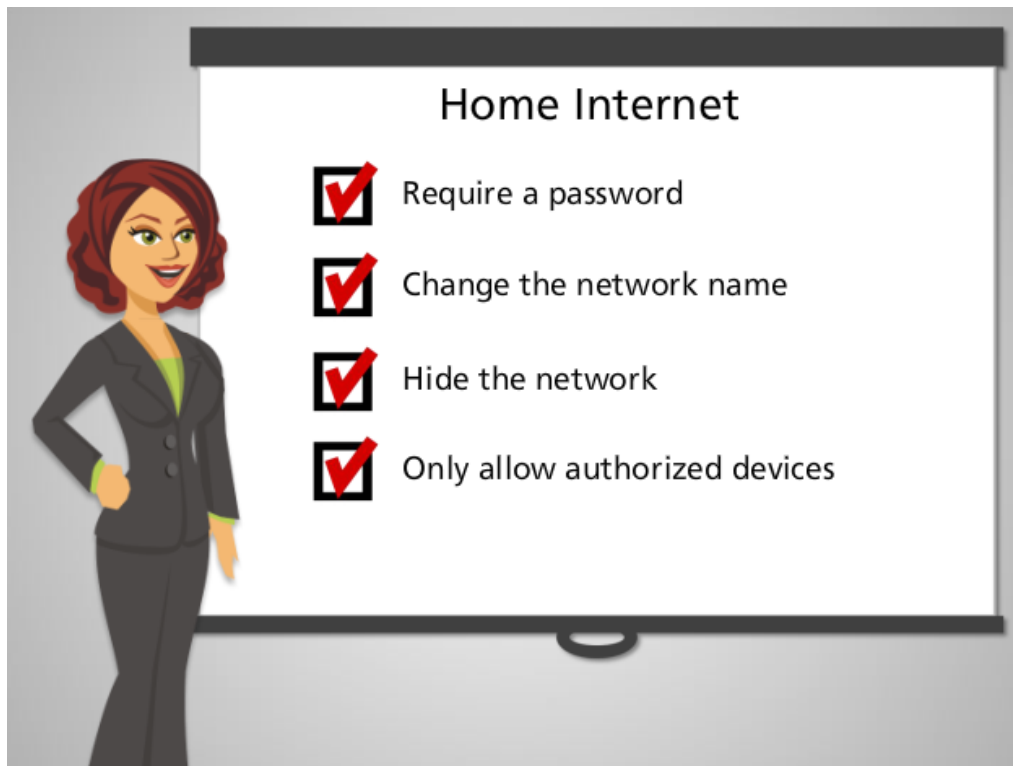
The way you connect to the internet also affects your level of privacy.

Some internet connections are secured and private, others are public connections that anyone can access.



Michelle usually accesses the internet from home. At times, she uses the free Wifi at her local coffee shop. She also uses the public computers at her local library.

Click on each type of internet connection to learn how to reduce your privacy risks.

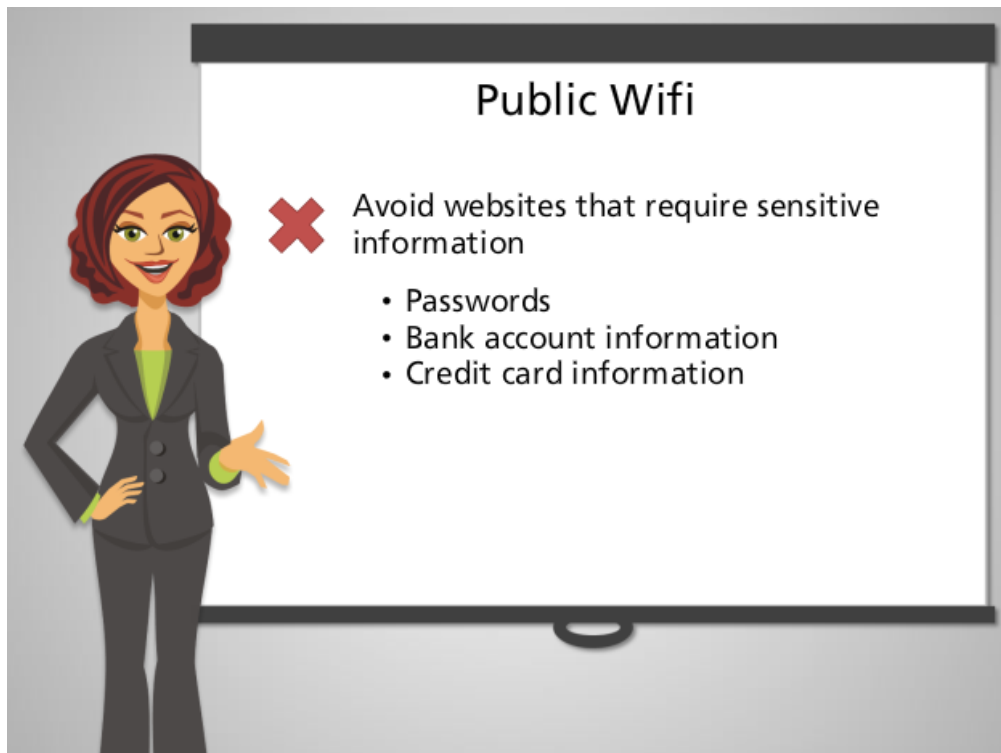


A home internet connection can be set up securely, or it can be open for anyone to connect to.

If your internet is not secured, someone might try to intercept information, such as our banking credentials, account passwords, and other valuable information. Neighbors would also be able to use your connection, making it slow.

To protect against this, you can secure your home internet connection by requiring a password to get on, changing the network name, hiding the network from view, or only allowing authorized devices to connect.

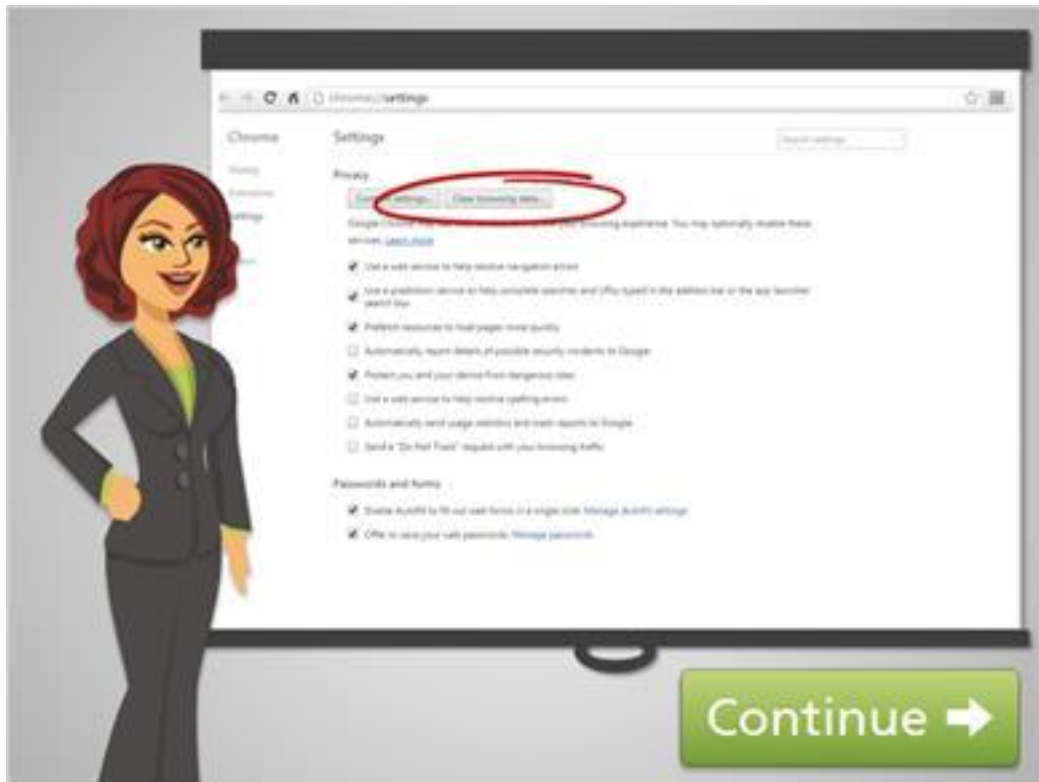
To learn how to configure your home network, visit onguardonline.gov. The steps are different depending on what equipment you use.



Free wifi is often available in coffee shops, airports, shopping malls, and other locations. While this is convenient, it can be unsafe **e if you aren't** cautious. Those who are looking to intercept and steal private data will often use public wifi.

You can take several steps to be safe on public wifi. First, make sure your computer has a personal security system, known as a firewall, enabled. For more on firewalls, visit [NEED SOURCE](#). Next, check with the location owner that the free wifi connection is legitimate. Then, make sure that any site you use has a secure connection before entering any personal information. To see if a website is secure, check for the HTTPS in the address bar.

It's a good idea to avoid accessing websites that require you to enter sensitive information, like passwords, bank account information, or credit card information over public wifi. Remember, anyone can access a public wifi connection.



In general, public computers at libraries and community computer centers have secure networks. A primary security concern involves other people **using the same computer after you've finished using it.**

When using public computers, make sure that private information is not **saved on the computer when you're done. Log out of any accounts you've** logged into before closing the browser window. You can also clear the history in the web browser, which will delete the list of websites you have visited. Delete any files that you might have saved on the computer.

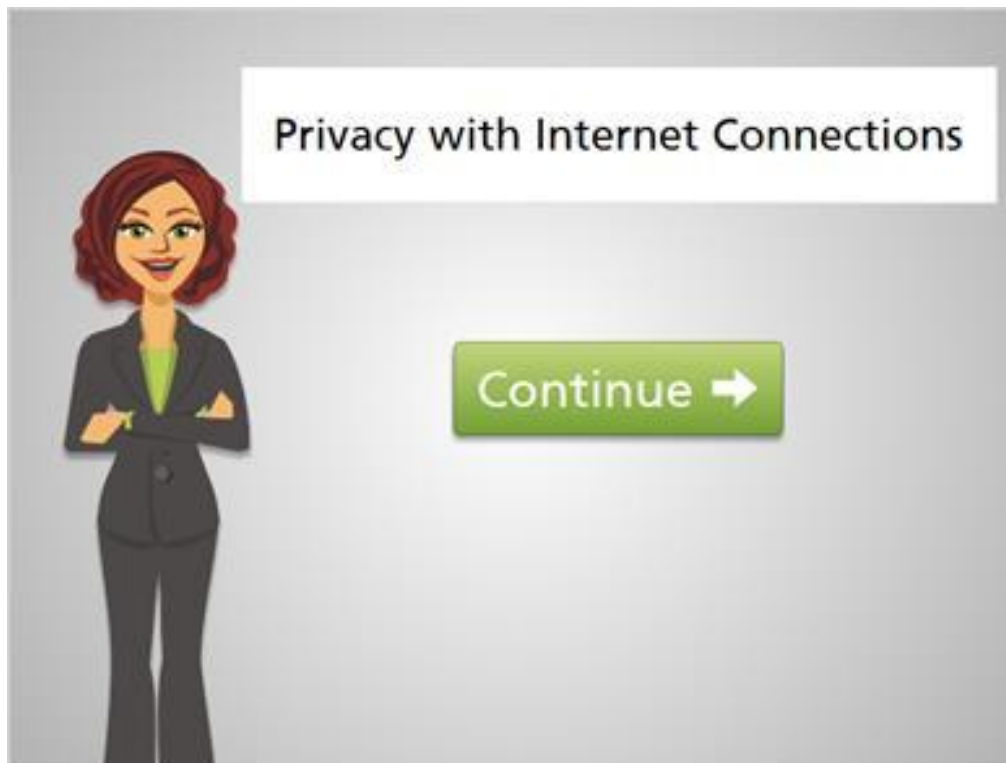
Note that most library computers have software that automatically remove **any personal browsing history and files saved to the computer, but it's a** good practice to ask the library staff to be sure before relying on it.

The best way to ensure your safety when using public wifi at a coffee shop is to avoid accessing websites that ask for personal information.

True

False

The correct answer is True.



No matter **where you're accessing the internet**, it's important to keep privacy in mind. Follow the tips in this course to stay in control of who can see what you're doing online.