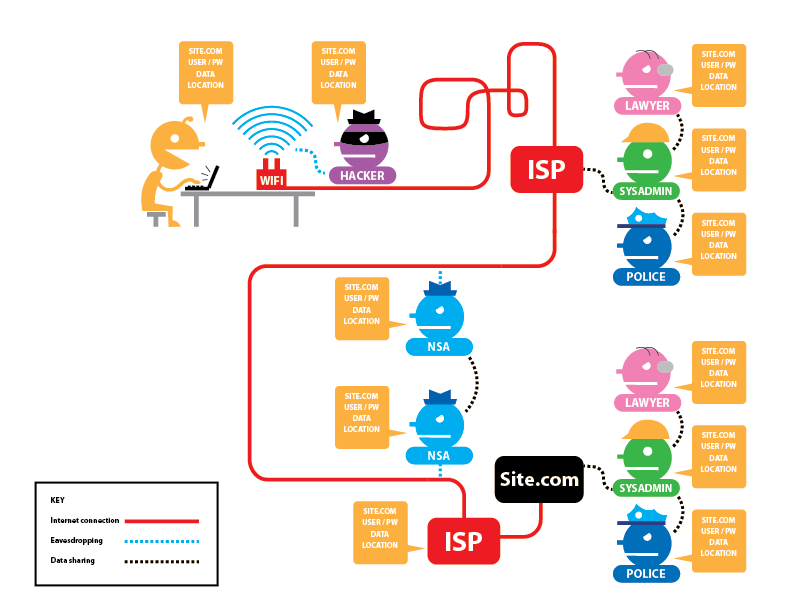
[SECURE CONNECTIONS](https://tb-manual.torproject.org/secure-connections/)

If personal information such as a login password travels unencrypted over the Internet, it can very easily be intercepted by an eavesdropper. If you are logging into any website, you should make sure that the site offers HTTPS encryption, which protects against this kind of eavesdropping. You can verify this in the URL bar: if your connection is encrypted, the address will begin with “https://”, rather than “http://”.

The following visualization shows what information is visible to eavesdroppers with and without Tor Browser and HTTPS encryption:

* Click the “Tor” button to see what data is visible to observers when you're using Tor. The button will turn green to indicate that Tor is on.
* Click the “HTTPS” button to see what data is visible to observers when you're using HTTPS. The button will turn green to indicate that HTTPS is on.
* When both buttons are green, you see the data that is visible to observers when you are using both tools.
* When both buttons are grey, you see the data that is visible to observers when you don't use either tool.

HTTPS   
Tor 



POTENTIALLY VISIBLE DATA

**Site.com**

The site being visited.

**user / pw**

Username and password used for authentication.

**data**

Data being transmitted.

**location**

Network location of the computer used to visit the website (the public IP address).

**Tor**

Whether or not Tor is being used.