How Secure is Your Internet Usage?

HTTP, HTTPS, and VPN Explained for Non-Technical Audiences

By Waqar Mahmood

Three terms we commonly hear when discussing information security over the web are HTTP, HTTPS, and VPN. Let us compare these three methods.

HTTP Protocol Explained

Consider the steps to write the address on an envelope in the U.S in English. The first line is the recipient's name. The next one or two lines have the street address. The next line has the city, state, and zip code. This format is an example of a protocol. Anyone who wants to send a letter knows how to address it so others understand where it is to go. Anyone handling the letter knows how to interpret the information the sender put on it.

Just as we use languages and protocols to communicate, so do computers. HTTP (hypertext transfer protocol) is a language or protocol that computers use to exchange information over the web. Any computer sending information over HTTP formats it so that receiving computers know how to correctly interpret what was sent.

HTTP Not Secure

Imagine you work from home and your colleagues work at an office building. Suppose you use a service called Public Delivery Service (similar to the postal service) to exchange documents with your colleagues. You put information you are sending inside a clear plastic *unsealed* envelope that has the name of the intended department. Suppose you have an envelope that is addressed to Accounting, and a memo inside the envelope names a specific recipient in the Accounting department. A delivery person comes to collect the envelope and delivers it to the intended department, which eventually routes it to the specific person when one is named. This delivery person brings to you any envelopes addressed to you, which are also unsealed clear plastic envelopes.

Sending information using HTTP over the internet is akin to the arrangement described above. The web address specifies where your information (e.g. you filled out a web form) or request (e.g. you are looking up local weather information) should be delivered. The website is the department to which you are sending information. Individuals within the department are similar to individual pages within the website. The provider of your internet service is the delivery person.

Using HTTP means that your internet provider or anyone else who has a way of seeing your information (like someone who is listening in on your internet connection) can read the

information you are exchanging. The information is in English and they can easily decipher the contents. They can see which websites and which pages within these websites you are visiting, as well as the information you are exchanging with these pages (e.g. which searches you did, information you entered).

HTTPS is Secure

HTTPS stands for hyper text transfer protocol secure. It adds a security mechanism to HTTP. Let us return to the office scenario to understand the benefit of HTTPS.

Suppose you need confidentiality. So you begin to write your information using a secret code. This code is known to the Accounting department but not to others. Now any third party with access to your envelope simply knows that you are sending information to Accounting. They cannot make sense of the envelope contents or who within Accounting is getting your documents.

Using HTTPS is similar to the arrangement above. Your internet provider or any third party who accesses your information may see which websites you are visiting. It sees neither the information you are exchanging (because this information is encrypted) nor the individual web pages you visit within the website.

The distinction between HTTP and HTTPS matters because not all sites, and not all pages within a website use HTTPS. Your information may be intercepted when you use HTTP.

Your browser will tell you whether you are using an HTTP or HTTPS connection. Below is an image of Google Chrome web browser showing an HTTPS connection to website amazon.com:

Notice that the HTTPS connection is shown as secure with a green lock, and it shows the https in the address bar. The image below shows an HTTP connection to website imdb.com

The i in a circle instead of the lock indicates that the connection is not secure. If you go the address bar to copy the www.imdb.com address and then paste it, you will see the pasted text to be http://www.imdb.com/.

Encryption Explained

HTTPS uses encryption to achieve security. Let us look at an example of encryption to see how it works.

Suppose you want to send your credit card number to your friend by email. You agree beforehand that you will add 2 to each digit of your credit card number. Your credit card number is 1234 1234 1234 1234 and you send 3456 3456 3456 3456. Your friend knows that you have added two to each digit so they subtract two from each digit to decrypt what they receive and obtain the correct number.

What you have done above is a very basic form of encryption. Encryption uses a secret code to modify information that is being sent so that it is difficult for anyone who does not know the secret code to decrypt and understand what was sent. A website that supports HTTPS uses an advanced technique to encrypt data that is exchanged with that website.

Security over VPN

VPN stands for virtual private network. The internet is a shared network. Your internet information travels over WiFi and/or cables and fibers that are shared by many users. Some of these users have the skills to listen in on information that is going over theses information pathways.

Suppose you lay down a private cable between your office building and your home. Now you have a private network or connection between your office and your home. It is harder for someone to access your information now because they don't have access to your private cable.

A VPN tries to mimic this private network without laying down a private cable. Let’s return to the office scenario to see how a VPN works.

Suppose you learn to your discontent that Public Delivery Service is keeping records about your mailing practices: to which departments are you sending mail, how often, etc. You contact another delivery company who promises not to keep records. Let’s call this company Private Delivery Company. Private Delivery Company comes and collects the information you need to send and transports it to its office. It then sends it through the Public Delivery Service to

Accounting. Accounting uses Public Delivery Service to send any responses intended for you to the Private Delivery Company. Private Delivery Company brings that information directly to you. Now your information is exchanged in a secure manner and the Public Delivery Service does not have information about your mailing practices.

A VPN provider is similar to Private Delivery Company. You install VPN software on your computer. You enter a web address in the address bar of your browser as you ordinarily would. The VPN software controls all internet traffic going in and out of your computer. It takes the web address you entered into your browser and sends it to its VPN server (a host computer that is maintained by the VPN company). This host computer then connects to the desired website on your behalf. It collects the response of the website and sends it back to your computer. The VPN software installed on your computer receives this response and displays it in your web browser. So you don't exchange information with websites directly, and it all goes through your VPN.

VPN offers the following benefits over use of HTTPS:

1. HTTPS only protects information you exchange via your web browser. VPN protects all information going over the internet: e.g. browser use, voice over internet, instant messengers, etc.
2. Any information you exchange with HTTP websites from a public location (e.g. coffee shop with a public unsecure connection, which is particularly susceptible to eavesdropping) is protected as it enters or leaves your computer.
3. Your internet provider does not know which sites you visited. Internet providers may keep records on your internet usage and sell this information to vendors.
4. You could potentially overcome geographical constraints. For example, if you are on travel overseas and need to order flowers from a website that blocks non-U.S. IP addresses, you might be able to access this site using a VPN that has U.S. IP addresses.

Many employers provide a VPN connection to their employees to allow them to connect with the company network from outside the office building. There are multiple companies that offer a private VPN service.

Summary

HTTP is an insecure protocol used to exchange information over the web. Anyone with access to what you send can see all information you exchange. HTTPS is safer because it encrypts the information you send via a web browser. Third parties can now only see which sites you visit. A VPN mimics a private network and protects even internet information that is sent without using a browser. All information you send goes securely through the VPN service provider. Thus even your HTTP connections are protected at your end, and your internet service provider does not know which sites you visit.