UNDERSTANDING HTTPS

As the internet has become more and more ingrained in our daily lives, experts have offered several wise pieces of advice on how to browse safely. There are countless articles, white papers, blog posts, and webinars about data security. Almost everyone keeps anti-malware software installed and up-to-date on their computers, both at home and at the office. Many have learned that, although perhaps inconvenient, it is wise to change your passwords regularly to protect yourself from hackers. And the average user is much more aware of phishing schemes and email fraud than they were ten years ago. But there is one security standard that many average users follow without even realizing they are doing so, mainly because the work is put in by the companies with whom they are doing business.

Although they may not know what it means, most people are used to seeing the “http” prefix at the beginning of most website addresses. What they may not realize is that on sites that deal with sensitive data—banking websites, e-commerce sites, medical and insurance pages, and the like—the prefix usually changes to “https.” That extra “S” stands for “secure,” and it represents significant work to keep your data safe.

https://www.paypal.com

An example of a secure web page

What does HTTPS do?

More specifically, HTTPS represents encryption. It follows the standard HTTP protocol that websites use to distribute content across the Internet, but covers it in a layer of encryption to prevent criminals from accessing your passwords, credit card numbers, and other sensitive information.

To make sure that the data you send is secure, HTTPS creates a secure connection with a Secure Socket Layer (SSL) between your computer and the server running the website that encrypts and decrypts the communications. The SSL layer is there to verify that your computer is talking to the right server (rather than an imposter). Beyond that, its purpose is to make certain that only you can read the information the server sends you, and that only the server can read the data you send.

SSL Certificates

SSL certificates are very small data files that are used to prove the website you’re visiting is actually the website it claims to be. In order to begin a secure session with web browsers like Chrome, Firefox, and Microsoft Edge (formerly Internet Explorer), organizations need to install an SSL certificate onto their server. This SSL certificate includes two “keys,” which are long sequences of randomly generated numbers. Without these keys, the encrypted data will be meaningless, so even if a hacker were to intercept the data, they wouldn’t be able to do anything with it. It’s an added layer of data leak protection, because the data can’t be translated until it’s safely on the server or your personal computer.

Public Keys and Private Keys

Many SSL certificates utilize both a public key and a private key. The two keys are mathematically linked to each other through complex algorithms. When HTTPS encrypts your data, it uses a public key to turn that data into what would be
gibberish to anyone without your private key. The private key only exists on your end of the communication, and it is what HTTPS uses to translate that gibberish back into useful information. Because your computer is the only one with your private key, you are the only one who is able to access your information. This all may sound complicated, but most users don't have to worry about it, because it all happens behind the scenes after organizations secure their websites.

The Benefits of HTTPS

Any organization that transmits private information over the internet should implement HTTPS to keep their data secure. In fact, many experts are now saying that all websites should implement HTTPS, whether they collect sensitive data or not. Not only does it build a higher level of trust with visitors, but search engines like Google will give preference to websites that utilize it than others. Customers want to know that their data is safe, and HTTPS is just one more way that organizations can assure their customers that data is in good hands.

Carol Evenson is a business consultant specializing in cybersecurity and data management. She has worked with Fortune 1000 companies and currently assists organizations within the US and UK.