THE JOURNALIST SURVIVAL GUIDE

AN ANIMATED VIDEO GUIDE

Samir Kassir eyes

Lesson 8

How to Get a Secure Connection?

Why this matters

While making sure that having a clean operating system is an important first step, it is important to ensure that any communications you conduct on your computer are transferred safely. This lesson will discuss how to verify a safe browser connection, as well as how to utilize a safer internet connection through an anonymizing proxy known as Tor.

What is HTTPS?

When communications take place between you and a site you are visiting, it is through the Hypertext Transfer Protocol (HTTP), which is the protocol used by browsers that allow this communication to take place.

The information that is communicated is sent in plain text, much like sending a postcard with personal information in the message. Data, such as usernames and passwords, sent to and received by Web sites, are easy to read by third parties. To solve this problem, the Hypertext Transfer Protocol Secure (HTTPS) was invented to provide encrypted communication and secure identification of a network web server. This changes your communications from being transmitted as if they are a postcard to a letter sealed in an envelope.

Most major Web sites, including Gmail, and popular social networking platforms such as Facebook and Twitter, can also be reached via a secure connection, but not necessarily by default.

You can check the settings in these platforms to enable HTTPS (or SSL, another way that this secure connection is referred to by default). However, to make this process easier, you can add in the plugin HTTPS Everywhere to the Firefox or Chrome browsers, which will automatically retrieve the HTTPS version of the websites you visit, such as Facebook, Twitter, etc.

It is important to note that HTTPS Everywhere will not create an HTTPS connection for all websites, only those that have an HTTP and HTTPS setting. Thus, it is still important to check the web address bar at the top of your browser to be certain that the websites where you must enter important information (email address, password, credit card information, etc.) is HTTPS enabled.

What is a Certificate?

A certificate can be thought of as the ID for a website, and it ensures the security of an HTTPS connection. Sometimes, your Web browser will show you a warning message describing a problem with the site›s digital certificate. These warning messages exist to protect you against attacks; please don't ignore them. If you ignore or bypass certificate warnings, you may still be able to use a site but limit the ability of the HTTPS technology to protect your communications. In that case, your access to the site could become no more secure than an ordinary HTTP connection.

If you encounter a certificate warning, you should report it by e-mail to the Webmaster of the site you were trying to access to encourage the site to fix the problem.

If you're using an HTTPS site set up by an individual, such as some kinds of Web proxies, you might receive a certificate error because the certificate is "self-signed", meaning that there is no basis given for your browser to determine whether or not the communication is being intercepted. For some such sites, you might have no alternative but to accept the self-signed certificate if you want to use the site. However, you could try to confirm via another channel, such as e-mail or instant messaging, that the certificate is the one you should expect, or see whether it looks the same when using a different Internet connection from a different computer.

If, however, you receive a certificate error for a common website, such as Gmail or Facebook, do not proceed!

Circumvention: What is it?

Circumvention is a way to get around any filters that are imposed by your internet service provider (ISP). These rely on one or more "proxies", which route your internet connection through a connection outside of the control of your ISP to the website that you wish to access.

Types of circumvention tools

Web Proxies

A web-based proxy is a service in which you type in a website for a particular proxy service at the web address bar at the top of the browser, and within the website, enter the filtered address you wish to view. The proxy will then display the requested content inside its own webpage.

While these types of proxies are the easiest to use, these only apply to your browser-based activities, and will not work with chat or email clients (Outlook, Skype, etc.). Also, not all web-based proxies will use an HTTPS connection to route your internet traffic.

It is important to remember that not all web-based proxies can be trusted. In some cases, groups who might wish to gain access to user account information may set up a web-based proxy, which would allow them to see all of your internet activities. Thus, it is important to use these services that are developed by entities that you can trust.

Virtual Private Networks (VPNs)

A VPN (virtual private network) utilizes an HTTPS connection and tunnels all Internet traffic between yourself and another computer. Because VPN services tunnel all Internet traffic, they can be used for email, instant messaging, Voice over IP (VoIP) programs like Skype, and any other Internet service in addition to Web browsing, making everything that travels through the tunnel unreadable to anyone along the way.

If the tunnel ends outside the area where the Internet is being restricted, this can be an effective method of circumvention, since the filtering entity/server sees only encrypted data, and has no way of knowing what data is passing through the tunnel.

Much like a web-based proxy, it is important that you trust your VPN provider. While there are no-cost solutions such as Psiphon 3 and commercial solutions through Amazon Web Services and other cloud-computing providers, these services will still be able to see what websites you access, even though your ISP will not be able to.

Anonymizing Proxies

The most secure type of proxy is an anonymizing proxy, which routes your internet connection through a series of 3 or more other proxies. The most well-known of these is Tor.

Tor randomly routes your communications through a network of independent, volunteer proxies. All the traffic between Tor servers (or relays) is encrypted, and each of the relays knows only the IP address of two other machines – the one immediately before it and the one immediately after it in the chain.

Tor makes it very difficult for:
your ISP or any other local observer to know what your target Web site is or what information you are sending
the target website to know who you are (or at least, to know your IP address)
any of the independent relays to know who you are and where you go either by directly having your IP address or by being able to correlate browsing habits by consistently observing your traffic.

To learn how to install and use Tor, please visit the following website: *https://securityinabox.org/en/tor_main*

Produced by:
The SKeyes Center for Media and Cultural Freedom at the Samir Kassir Foundation

The content of the video was prepared with the pro bono assistance of:
The ICT team at the National Democratic Institute

Executive producer: **Maroun Sfeir**
Storyboard creation and animation: **kook creative studio**

Video Consultant: **Andrew Codd**
Translation: **Nour El-Assaad**
Voice over - Arabic: **Rima Khaddaj**
Voice over - English: **Andrew Codd**
Sound recording: **Creative Impact**
Music: **“Mining by Moonlight” by Kevin MacLeod**

This project has been made possible thanks to the support of the **National Endowment for Democracy**.