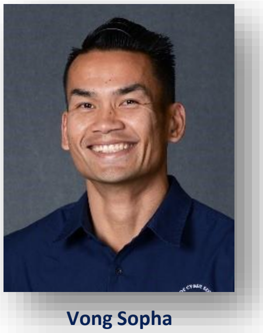
The CYBER GURU

SAN DIEGO COUNTY OFFICE OF EDUCATION



Vong Sopha
Cybersecurity Analyst

The moment you are online and viewing a website, you are transmitting information from your computer to the web server and from the web server to your computer. When these transmissions send information through HTTP instead of the secure HTTPS, your information is being sent in plain text.

This may not be an issue if you are merely browsing or reading news articles on websites. Most users, especially during the holidays, prefer to do their shopping online, and therein lies the problem. If any website or web page requires you to give your information, make sure the site is using HTTPS, which is a revision of the HTTP for a secure communication over a network on the internet. While using HTTPS, your information in transit is encrypted and eavesdroppers or hackers will not be able to figure out what that information is. It is critical that you check for a secure connection while proceeding with your online shopping, since most sites require you to enter your home address, phone number, credentials, and credit card number. This can easily be done by viewing the address bar on your browser to make sure the address has a lock icon and "https" before the web address.

Online criminals can easily intercept your web traffic with an array of exploits, which can include address resolution protocol (or ARP) spoofing, a man-in-the-middle (or MINM) attack, or a secure sockets layer (SSL)-stripping tool. Here is a quick scenario: You are at a coffee shop and connect your mobile device to the free Wi-Fi provided by that establishment. Now the hacker or online criminal also connects to the same free Wi-Fi. At this time, both of you are now on the same network. The hacker uses a tool called ARP-spoofing that allows him to pretend that he is the gateway of that network. The gateway or router address is a checkpoint all network traffic must pass through to get on the internet. Now that the hacker has successfully told your mobile device that they are the gateway, all of your traffic will now pass through them. If that traffic is not encrypted with HTTPS, the hacker will be able to see everything in plain text. This is one form of a man-in-the-middle attack. Another method or tool that hackers are using is called a stripping SSL or HTTP-downgrading attack. Again, we will stick with the same scenario of the free Wi-Fi and coffee shop. In this situation, the hacker has already established themselves as the gateway between you and the web server. You log into Amazon.com, which is secured. The hacker passes this information along to Amazon, which then responds back with an HTTPS secure login page. The hacker captures that traffic then strips the "S" from the original response and sends a HTTP login request to the victim. If the victim was not carefully attentive of the web address, they type in their username and password for the unsecured HTTP request, which results in giving their username and password to the hacker. Any web pages asking you for any information should be secure.