Protecting Your Communications on Public Networks

There are many ways in which your personal computer can be compromised when on public Wi-Fi. One main way is in which your communications are intercepted by a malicious third party in what is known as a man-in-the-middle attack(MITM). One way to explain MITM is as follows: Imagine you're in a meeting and you wish to pass notes to a colleague. In order for your notes to reach your colleague other, potentially malicious, colleagues must relay your message. During this process they can open your note in which they can read the contents and modify them in any way, potentially causing you lots of grief! Public Wi-Fi MITM attacks work the same way. So how do you protect yourself?

Going back to our original analogy one way to protect yourself is to put your note in a security lock box that only your friendly colleague knows the combination to. Another possibility is to even use a cipher such as pig-latin if your malicious colleagues don't know it! The basic idea is to render useless any information a "man in the middle" could obtain. In the technology world there are several tools and technologies available to do this for you. One such tool that makes all of your web browsing history appear to be "pig-latin" is HTTPS Everywhere. HTTPS Everywhere is a freely available add-on for your web browser provided by the Electronic Frontier Foundation at https://www.eff.org/Https-everywhere. Another tool available to UTHSC employees is to use a Virtual Private Network(VPN). A VPN in our original analogy is that of a security lock box. All of your information is locked away until it reaches the safe, protected UTHSC network. Details on how to install and use a VPN on your computer are available at:
https://www.uthsc.edu/helpdesk/vpn and
https://www.uthsc.edu/helpdesk/vpn/mac_instructions.php respectively.