NETWORKING

Summary/Overview

Networking explores how computers speak to one another and the programming necessary to maintain its functionality. Networking relies on the use of HyperText Transfer Protocol (HTTP), domain name systems, TCP/IP, and the physical infrastructure. On a network that has the proper setup, there are several methods of interaction, but the most common involves the use of servers.

As a user interacts with a server, requests are made using methods, with the most common including “GET” and “POST”. These requests are the backbone of servers, allowing back end users to modify and make changes to content and functionality and front end users to interact with the current systems. When a request is completed successfully, the server returns a 200 status code. When requests are unable to be completed, users will receive a 300 (something else must be done first), 400 (the front end user made a mistake), or 500 (an error on the server end) status code.

Proposal for Assimilation in Current Curriculum

One of my favorite units to teach in my class is my Cybersecurity unit, and while the unit itself is typically covered in two to three weeks, the students explore a multitude of material in a short amount of time. The earlier lessons explore news articles and internet safety/digital citizenship, which leads into the construction of a Raspberry Pi computer and the programming of IP addresses inside of the Terminal on the device. In later lessons, students then set up a local computer network that allows them to exchange information between two of the constructed devices. The last activity has students create encrypted messages, which are then sent over the computer network they created and decrypted using specific ciphers (simulating hacking).

The best lesson to include networking in this unit is easily when the students begin working with the Raspberry Pi computers and setting up the private computer networks. The inclusion of how a server works would be incredibly helpful as cybersecurity relies on the proper functionality of servers on the Internet. Since students mostly interact with front end services on websites, the knowledge of how everything operates behind the scenes would help a number of students potentially explore careers in STEM.

Proposal for Instruction in Current Classroom

There is a high probability that students will struggle with networking as the Cybersecurity unit is easily the most challenging unit for students to complete. Students in my past and most recent classes often have questions varying greatly between the programming, setup, and hardware assembly. The current curriculum may even be too difficult for these students, and the addition of further concepts could potentially have adverse effects on their skill development.

However, exploring networking in greater detail may assist students with understanding the foundation of the work they do on the cybersecurity side. As such, the activity proposed would require students to set up their own server in the form of a website or app, which would run completely offline to ensure a safe simulated environment. This activity would be included alongside exploring how networks are created and how IP addresses are then integrated into these networks. Once these servers are created and the foundation is established, the original activity involving hacking would evolve into a much more intense process. For this activity, half of the students would act as the “hackers” and simulate a cyberattack on the servers that students created earlier, while the other half would attempt to fight off the cyber attackers. As middle schoolers are motivated immensely by competition, providing prizes to the winning side would be included, but the main goal would be to reflect on what takes place during the process in an effort to show students how they can protect themselves from similar attacks. This may also encourage students to pursue cybersecurity as a career, which is important since it is a career field high in demand.