Course: CSCI 450 / ECE 461 – Software Engineering
Assignment: Homework 1
Section : **#6**
Description: Tokens Group Discussion

As brought out in the GitHub documentation, a token functions as a stand-in for your password. This means that anyone with access to your personal access token essentially has access to your signature (*"Managing Your Personal Access Tokens"*).

Tokens are used for authentication and authorization. When these tokens are made public, this facilitates a sort of impersonation of the actual owner. This allows bad actors the ability to delete important repos, change code,modify GitHub Actions pipelines, or view critical information. In fact, if a token is exposed, unauthorized users could gain access to any GitHub repository linked to the associated account. One could argue that infiltrating a repo of college class material is a small issue. However, in an enterprise environment there could be much bigger repercussions. After gaining access to a stolen token, interlopers have an opportunity to figure out the inner workings of a system and use that information to exploit the application and its users.

Source:

GitHub Article – "Managing Your Personal Access Tokens"
https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/managing-your-personal-access-tokens

This response was the result of collaboration between all 6 members of Team 1. Each member contributed.