Hello everyone! While I understand security concepts, implementing those concepts still seems greatly foreign to me, lol. One-way operating systems are able to prevent unauthorized access is through log-on protocols, that require a user to have a unique user identification and unique complex password. Another way an OS prevents unauthorized access is through use of policies that prevent files from being written to, unless the person currently accessing the file is the owner and/or has write permission for the files on the system. More sensitive files, such as system files containing configuration information goes a step further, denying all access, including view access, unless you are logged in with administrative credentials and permissions. Having security protocols and procedures in place on an any type of technology that is network connected, MUST have security in place that provides different users with different levels of access, enabling the system to grant or deny a user access to specific parts of the data contained within, and is one major way an operating system contributes to keeping data secure.

There are countless ways for people with malicious intent to access your information. Some include address spoofing, buffer overflow attacks, reconnaissance attacks, and malware. There are ways to make your information safer, such as flag alerts being in place, set with software made to monitor suspicious activity or access attempts for sensitive information. A necessary countermeasure that should be implemented when viewing, exchanging, and storing sensitive data is encryption, along with limiting access on a “need to know” level of clearance and permissions in tandem with secure firewall settings, malware, and anti-virus detection, protection prevention that does not get turned off, thus it is constantly monitoring your system and the data contained within it. While these measures will help deter unauthorized access, there is no way to truly prevent future invasions, as tech is always changing, the methods hackers use to gain access to our information is as well. But, changing passwords regularly, not having the same password for multiple applications, making passwords complex through inclusion of different cased letters, numbers, and characters while avoiding sequences such as (1, 2, 3 or ABC), repetitions (zzz, 111), or personal information for passwords that give you access to sensitive information is likely the most helpful countermeasure an individual can take to keep sensitive material that they have access to secure.

The best way to handle authorization is to understand that it is not a singular process, at least when it is done correctly and securely. Authorization needs to be paired with authentication, to ensure that access already given, isn’t being used by an unauthorized person or entity. I like to think of it like my debit card. Even having a PIN, my name on the card, and unique, one of a kind card number does not mean my account is safe, does it? NO, it is still secure for a plethora of reasons. Most card readers in use today, have the option to run a debit card as credit, thus circumventing the need of knowing the cardholders PIN, and I do not know anywhere anymore that requests you show them your id before running your card, and there are numerous ways for people to gain access to your card number, with use of algorithms, AI, and number generators. Then there is the issue of, say your 16-year-old daughter, wanting to buy something, thinking you will not check bank statements, which leads her to make an online purchase with your card… not that I have had that happen…(sarcasm). Without authentication, preferably multi-factor, authorization alone is simply ineffective. So, to my point, sorry, I tend to go down the rabbit hole sometimes, so to speak, lol, using a need-to-know level of authorization for access, along with layering your levels of authentication is the best way to handle authorization.

Lastly, the only thing I think I did not cover is data loss and ways to prevent it. BACKUP!! BACKUP!! BACKUP!!! Save your work as you go, to a secure, yet separate location that allows you access to version control. For any unfamiliar with version control, it is a life saver! When facing a problem with a development, I tend to just drudge on until I find something that works… But even after it works, being a perfectionist, I go to tweaking the program to implement another feature I just thought of, or I think there is a way to improve runtime, and so on. Only, after making a change, I do something that crashes the entire program. Version control allows users to go back to a version of the file, before the edit that crashed it was made, convert the program back to its previously running state. It also helps developers or team members look through the stages taken to develop the program, which can offer keen insight and show clarity on how to perform or implement a process. In conclusion, making sure you have a secure way to backup, access, store, and restore your information will prevent data loss. While data loss may not immediately appear as a security concern, it absolutely should be. For someone could intentionally remove data with malicious intent, such as protocols put in place to keep your system secure, or even as a result of negligence be leaked, making it accessible to those without authorization, which is just one scenario of why data loss prevention has an important and relative relationship with data security.