**Discussion Question: SQL**

For this module's discussion board assignment respond to **one**the following topics:

1. You run a query on the mysql.user table and find user accounts with the hostname listed as "%". What does this mean, and what concerns might that cause?
2. Would you create a user with a blank password? Why or why not?
3. What would be the reason for granting permissions to a user and then immediately revoking those permissions?
4. How often should users and their permissions be monitored? Why?

     A program can have a wide range of functions and information. When developing a program, it is vital to remember that not all users need access to the same information. There need to be parameters in place for users, and their permissions should be monitored.

User permissions should be monitored regularly. To keep the system as up-to-date as possible, I believe going through users’ permissions should at least be a monthly occurrence. If it is for an employee, the permissions should also be updated when there is a promotion, job title, or change of responsibilities. This could mean adding more access, revoking access, or a combination if specific permissions are no longer needed in a particular role. Unusual activity or security breaches could call for permission updates as well.

For example, roles are assigned to different users at my workplace, depending on their position. Since I am an administrative assistant and track hours, I have access to the project manager, sales representative, and personal employee center roles. In these roles, I cannot see private information related to other employees that go outside my range of what I am permitted to access. Before I started tracking hours, I did not have the needed permissions to take on the project manager role unitl I requested them.

**Reference**

Comeau, A. (2016). *MySQL explained: your step-by-step guide to database design*. Ostraining.

***Before you submit your thread, put your name in the subject line.***

**Assignment Requirements and Grading:**

1. An initial post is due by **Thursday, 11:59 p.m. CST**.
2. For the initial post to be considered substantive, it should fully cover the topic(s) being presented. Single-sentence definitions or responses will not be awarded points.
3. Submit your post by clicking on the **Assignment Link** above, then **Create Thread**. You must create a thread in order to view your peers' posts. Tip: Create your post in a Word document and then copy and paste your work into the thread.
4. A minimum of three (3) responses, **to the original threads of other students**,, of 100-200 words each are due by **Sunday, 11:59 p.m., CST**.
5. To view the rubric grading criteria, click on the following link: [Discussion Board Grading Rubric.](https://content.bellevue.edu/cst/csd/rubricdbv3.pdf)

**(50 points)**

Joe, I enjoyed reading your post and thought it was very insightful. You are correct that giving out permissions can be a significant risk to the entire database, so administrators must be mindful of the permissions they grant, who they grant them to, and how long they should be granted. It may seem confusing to the user with limited access, but it is the best course of action. I also agree with you that there must be options for temporary authorization of these functions for users other than the administrators. If a user is demoted, this may also lead to revoking the once-approved permissions.

Nardos, you did a fantastic job explaining your answer in your post. I agree with you that it is best practice not to create users with blank passwords. In my opinion, if a user does not require a password or utilizes a blank one, then there is no real reason for the option to create a user to exist. The negatives far outweigh the only benefit I find: convenience for the user. Anyone can gain easy access, causing harm to any private information that may be stored under the user, and the database is at risk for overall corruption. Even for a personal device, it is not the safe route to go.

Adrian, you did a nice job explaining what it means in MySQL if a user account has % as the hostname. Every week, I further understand the importance of maintaining proper security in databases and my overall systems. I really like your suggestion of using strong passwords! They are a great defense. Before this class, I did not realize that the % symbol performs as a wildcard. It makes me wonder if this is how virtual private networks work or if it is a different process. I know you can utilize VPNs to show that a user is at a different location, giving the user access to geo-blocked content.