Duo: Frequently Asked Questions

Question 1: What is Duo?

Answer 1: Duo is a multifactor authentication (MFA) tool created by Cisco.

Question 2: Why does ITS use Duo?

Answer 2: There are two main reasons:

1. MFA tools protect users from hostile agents trying to exploit state employee credentials. MFA has kept attackers from getting access to protected information.
2. The State Controller's Office (SCO) selected Duo as the MFA tool for Luma. ITS then used it for supported agencies to minimize the number of tools used and costs.

Question 3: How often should I be logging in?

Answer 3: Most users should authenticate once per day per device. This means users authenticate once per 24-hour period when logging onto computers, Microsoft 365 services, mobile devices, or rebooting devices.

Question 4: I don't need to log in once per day. Why is that? What should I do about this?

Answer 4: There are three reasons for infrequent logins:

1. **Duo rollout**. The initial Duo rollout set policies that only required users to authenticate once every 30 days or at password changes. These users have not been moved to the new policies yet.
2. **Policy configuration**. Initially, ITS created custom policies for users with different compliance requirements. Since then, ITS simplified the number of policies. A few users and two agencies were not moved to these new policies.
3. **Authentication problems**. Because of the number of authentication methods Microsoft supports, several processes may break during the authentication.

Question 5: Why do I have to Duo authenticate so often?

Answer 5: Users logging in more than once per day per device should contact the ITS Service Desk, as this may be a broken authentication process.

Question 6: What is ITS doing to make the Duo user experience better?

Answer 6: ITS is addressing this in three ways:

1. Working to get all supported agencies standardized as part of the Duo project.
2. Standardizing the Microsoft authorization configurations to simplify the user experience and reduce the number of problems that occur.
3. Addressing authentication problems as they arise.