# Password Checklist

*For information about **User Accounts**, including SJSU and CSUMB accounts, see the **User Accounts page** on the IT Website.*

*Keep in mind that your Gmail password is not necessarily the same as your MLML password.*

## Password Checklist

A strong and unique password will keep your account safe.
Here is a checklist for creating secure passwords for all of your accounts:

- Your password should be easy for you to remember without being obvious for someone else to guess.
- The **longer and more complex** the password, the stronger it is.
  - Include a variety of characters, such as punctuation marks, numbers, and mix capital and lowercase letters.
  - Don't choose a dictionary word as your password.
- Have a **recovery email** or **phone number** set up with your account to be able to recover it in case you lose access.
  - Here are the Google Account Recovery instructions.
  - If you ever have a situation where your account is compromised, check to see that the recovery email or phone number hasn't been changed.
- **Never use the same password** on multiple accounts. A **password manager** can help you keep track of your passwords (and generate very strong passwords).
- **Use multi-factor authentication**. This adds an extra layer of security by having you approve a login with your smartphone or entering a code sent to your smartphone or from a physical token.
  - Gmail 2-Step Verification instructions.
  - All SJSU employees must use Duo 2-Factor Authentication to access SJSUOne services. For instructions, see our Guide to set up Duo 2-Factor Authentication.
- **Never tell anyone your password**.
- **Never write down your password**. Use a **password manager** instead!
- Periodically **change your password**.
- Make sure you have strong passwords on all of your accounts.

---

Revision #19
Created 11 February 2019 23:37:43
Updated 16 September 2019 18:36:05